XUDOYKULOV Z.T., ISLOMOV SH.Z., MARDIYEV U.R.

# KRIPTOGRAFIYA 1

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

XUDOYKULOV Z.T., ISLOMOV SH.Z., MARDIYEV U.R.

# KRIPTOGRAFIYA 1

O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

Toshkent
“METODIST NASHRIYOTI”
2024

**UDK: 003.26.(075.8)**
**BBK: 32.973.2-018ya7**
**X 87**

**Xudoykulov Z.T.**
**Kriptografiya 1/ Islomov Sh.Z., Mardiyev U.R. /. O‘quv qo‘llanma. – Toshkent: “METODIST NASHRIYOTI”, 2024. – 216 b.**

O‘quv qo‘llanmada kriptografiya fan sohasi va uning axborot xavfsizligini ta’minlashdagi o‘rni, kriptografiyaning matematik asosi, klassik shifrlar va ularning tahlili, psevdotasodifiy sonlar generatori va ularga asoslangan simmetrik oqimli shifrlash algoritmlari, simmetrik blokli shifrlash algoritmlari, xesh funksiyalarni yaratish asosi va zamonaviy xesh funksiyalarning nazariy va amaliy asoslari muhokama etilgan.

O‘quv qo‘llanma 60610300 – “Axborot xavfsizligi (sohalar bo‘yicha)” yo‘nalishi bo‘yicha ta’lim olayotgan talabalar uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta’minlash bilan bog‘liq bo‘lgan mutaxassislarning keng doirasi uchun ham foydali bo‘lishi mumkin.

**Taqrizchilar:**

**K.A.Tashev** – texnika fanlari nomzodi, dotsent, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-ishlar va innovatsiyalar bo‘yicha prorektori.

**O.P.Axmedova** – texnika fanlari nomzodi, “UNICON.UZ” DUK – Fan-texnika va marketing tadqiqotlari markazi “Axborot xavfsizligi va kriptologiya ilmiy tadqiqot bo‘limi” boshlig‘i.

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligining 2021-yil 18-avgustdagi 356-sonli buyrug‘iga asosan nashr etishga ruxsat berildi.

**ISBN 978-9910-03-246-2**



## MUQADDIMA

*So‘ngi yillarda axborot kommunikatsiya texnologiyalari sohasining jadal rivojlanishi turli manbalardan tez va osonlik bilan axborot olish imkoniyatini taqdim etmoqda. Davlat muassasalari, tijorat korxonalari va jismoniy shaxslar masofadan turib axborot xizmatlarini taqdim etmoqdalar va ulardan foydalanmoqdalar. Turli ma’lumotlarni, to‘lov haqidagi ma’lumotlar, tashkilotga oid ma’lumotlar va shaxsiy ma’lumotlarni tarmoq bo‘ylab uzatilishi, foydalanilayotgan axborot tizimiga ma’lum xavfsizlik talablarini shakllantirish zaruriyatini qo‘yadi.*

*Shu sababli axborotni ishlash, uzatish, saqlash jarayonida uning xavfsizligini ta’minlash maqsadida, mazkur soha bilan shug‘ullanuvchi xodimlar jalb qilinmoqda va ishonchli himoya mexanizmlaridan foydalanishga alohida e’tibor berilmoqda. Ishonchli himoyani ta’minlashda matematik isbotga asoslangan mexanizmlardan biri – kriptografiya.*

*Keyingi yillarda kriptologiya yo‘nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. 2022-2026-yillarda mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasida “Kiberjinoyatchilikning oldini olish tizimini yaratish” kabi vazifalar belgilangan. Bundan tashqari, O‘zbekiston Respublikasi Prezidentining 2007-yil 3-aprelda qabul qilingan «O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-614-son Qarorida belgilangan asosiy vazifalardan biri axborotni muhofaza qilish sohasida yuqori malakali kadrlarni tayyorlashdan iborat bo‘lib, buning uchun axborot xavfsizligi va kriptografiya yo‘nalishlarida davlat tilida ta’lim olayotgan talabalar, tadqiqotchilar va ilmiy xodimlar uchun mo‘ljallangan o‘quv qo‘llanmalar, darsliklar, uslubiy qo‘llanmalar va kitoblar chop etish muhim ahamiyat kasb etadi. Mazkur o‘quv qo‘llanma ana shu sohada bajarilgan ishlardan biri hisoblanadi.*

*Qo‘llanmaning birinchi bobida axborot xavfsizligini ta’minlashda kriptografiyaning o‘rni, kriptografik funksiyalar, kriptografiyaning asosiy tushunchalari va atamalari, zamonaviy kriptografiyaning bo‘limlari haqida ma’lumotlar keltirilgan.*

*Ikkinchi bob kriptografiyaning matematik asosiga bag'ishlangan hamda ehtimollar nazariyasi asoslari, axborot nazariyasi asoslari, murakkablik nazariyasi, sonlar nazariyasi va fundamental algebra asoslariga oid ma'lumotlar keltirilgan.*

*Uchinchi bobda klassik shifrlash algoritmlari, xususan, sodda o'rniga qo'yish va o'rin almashtirish shifrlari, Vernam shifri, Kodlar kitobi, Enigma mashinasi va ularning kriptotahliliga oid ma'lumotlar keltirilgan.*

*Qo'llanmaning to'rtinchi bobi oqimli shifrlash algoritmlariga bag'ishlangan bo'lib, tasodifiy ketma-ketliklarni hosil qilish usullari, chiziqli va chiziqsiz kongurent generatorlar, oqimli shifrlarni qurish usullari hamda qator zamonaviy oqimli shifrlash algoritmlari haqida ma'lumotlar keltirilgan.*

*Beshinchi bobda simmetrik blokli shifrlarni qurish usullari, zamonaviy simmetrik blokli shifrlar standartlari, algoritmlari va simmetrik blokli shifrlash rejimlari haqida batafsil ma'lumotlar keltirilgan.*

*Yettinchi bob axborotning yaxlitligini ta'minlashga bag'ishlangan bo'lib, unda xesh funksiyalar va ularni qurish usullari, zamonaviy xesh funksiya algoritmlari, ma'lumotlarni autentifikatsiyalash kodlari haqida ma'lumotlar keltirilgan.*



# 1 BOB.
# KRIPTOGRAFIYA VA UNING FUNDAMENTAL TUSHUNCHALARI

## 1.1. Axborot xavfsizligi va kriptografiya

*Axborot* tushunchasi tushunilgan miqdorni anglatib, u turli ko'rinishlarda bo'lishi mumkin. Axborotni ishonchli himoyasini tashkil etishda kriptografiya muhim ahamiyat kasb etadi. Kriptografik himoyani joriy qilish uchun axborot xavfsizligi bilan bog'liq umumiy masalalarni tushunish kerak. Axborot xavfsizligi vaziyat va talabga muvofiq ravishda turlicha namoyon bo'ladi. Foydalanuvchining kimligidan va qanday darajada ishtirok etganidan qat'iy nazar tomonlar axborot xavfsizligi bilan bog'liq ba'zi maqsadlarga erishadi. 1.1-jadvalda ushbu maqsadlarning ba'zilari keltirilgan.

*1.1-jadval*

**Axborot xavfsizligining maqsadlari**

| № | Maqsad | Izoh |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Shaxsiylik yoki konfidensiallik | Axborotni ko'rish huquqiga ega bo'lganlardan tashqari barchadan sir tutish |
| 2. | Ma'lumot yaxlitligi | Axborotni ruxsatsiz yoki noma'lum vositalar bilan o'zgartirilmaganligini ta'minlash |
| 3. | Subyekt autentifikatsiyasi yoki identifikatsiyasi | Subyektning shaxsini tasdiqlash (masalan, shaxs, kompyuter, kredit karta va h.k) |
| 4. | Xabar autentifikatsiyasi | Ma'lumot manbasini tasdiqlash; u ma'lumot kelib chiqishi autentifikatsiyasi deb ham ataladi |
| 5. | Imzo | Subyektga axborotni tegishligini ko'rsatadi |
| 6. | Avtorizatsiya | Bir narsani qilish uchun subyektga ruxsatni yetkazish |
| 7. | Tasdiqlash | Axborot yoki resursdan foydalanish yoki boshqarishda avtorizatsiyani o'z vaqtida taqdim etish |
| 8. | Foydalanishni boshqarish | Imtiyozli subyektlarga resurslardan foydalanishni cheklash |

| 1 | 2 | 3 |
|---|---|---|
| 9. | Sertifikatlash | Axborotni ishonchli tashkilot tomonidan tasdiqlash |
| 10. | Vaqt belgisi | Axborotni yaratish yoki mavjud bo‘lish vaqtini qayd etish |
| 11. | Guvohlik berish | Yaratuvchidan boshqa subyekt tomonidan axborotni yaratilganligi yoki mavjudligini tekshirish |
| 12. | Qabul qilish tasdig‘i | Axborotni qabul qilinganligini tasdiqlash |
| 13. | Isbotlash | Xizmatlar taqdim etilganligini tasdiqlash |
| 14. | Egalik qilish | Subyektga resurslardan foydalanish yoki boshqalarga o‘tkazish uchun qonuniy huquqni taqdim etish |
| 15. | Anonimlik | Ba’zi jarayonlarda ishtirok etuvchining shaxsini yashirish |
| 16. | Rad eta olmaslik | Oldingi majburiyatlarni yoki harakatlarni rad etishni oldini olish |
| 17. | Bekor qilish | Sertifikat yoki avtorizatsiyani bekor qilish |

Asrlar davomida axborotni fizik ko‘rinishdagi hujjatlarda uzatish uchun axborot xavfsizligi masalalarini hal qiluvchi protokol va mexanizmlar ishlab chiqilgan. Axborot xavfsizligini ta’minlashda qo‘yilgan maqsadga erishish nafaqat protokol yoki algoritmlar asosida, balki muolajaviy usullar va ma’lum qonunlarga rioya qilish asosida ham amalga oshiriladi. Masalan, maktub va xatlarni yetkazib berishda maxfiylik pochta xizmati orqali taqdim etilgan muhrlangan konvert orqali ta’minlanadi. Bundan tashqari, konvertga jismoniy zarar yetkazish yoki ruxsatsiz ochish jinoyat sifatida baholanadi.

O‘z navbatida hozirgi elektronlashgan jamiyatda axborot xavfsizligiga erishish uchun ham ko‘plab texnik va huquqiy ko‘nikmalar talab etiladi. Shunday bo‘lsada, axborot xavfsizligining barcha yuqorida keltirilgan maqsadlariga yetarli darajada erishishning imkoni yo‘q. Aksariyat hollarda, axborot xavfsizligini ta’minlashda zarur bo‘lgan texnik ko‘nikmalar kriptografiya orqali ta’minlanadi.

*Kriptografiya* axborot xavfsizligining maqsadlari: konfidensiallik, ma’lumot yaxlitligi, subyekt autentifikatsiyasi va xabar autentifikatsiyasi, bilan bog‘liq matematik usullarni o‘rganadi. Kriptografiya nafaqat axborot xavfsizligini ta’minlash vositasi, balki



usullar to‘plami ham hisoblanadi. Kriptografiya 1.1-jadvalda keltirilgan axborot xavfsizligining quyidagi maqsadlariga erishishni kafolatlaydi:

*1. Konfidensiallik* – bu axborot mazmunini unga ega bo‘lishga vakolati bo‘lganlardan tashqari, barchadan saqlash xizmati hisoblanadi. Ko‘p hollarda maxfiylik tushunchasi konfidensiallik va shaxsiylikka sinonim sifatida ishlatiladi. Konfidensiallikni ta’minlashda fizik himoyalashdan tortib axborotni tushunarsiz holatga keltiruvchi matematik algoritmlargacha bo‘lgan yondashuvlardan foydalaniladi.

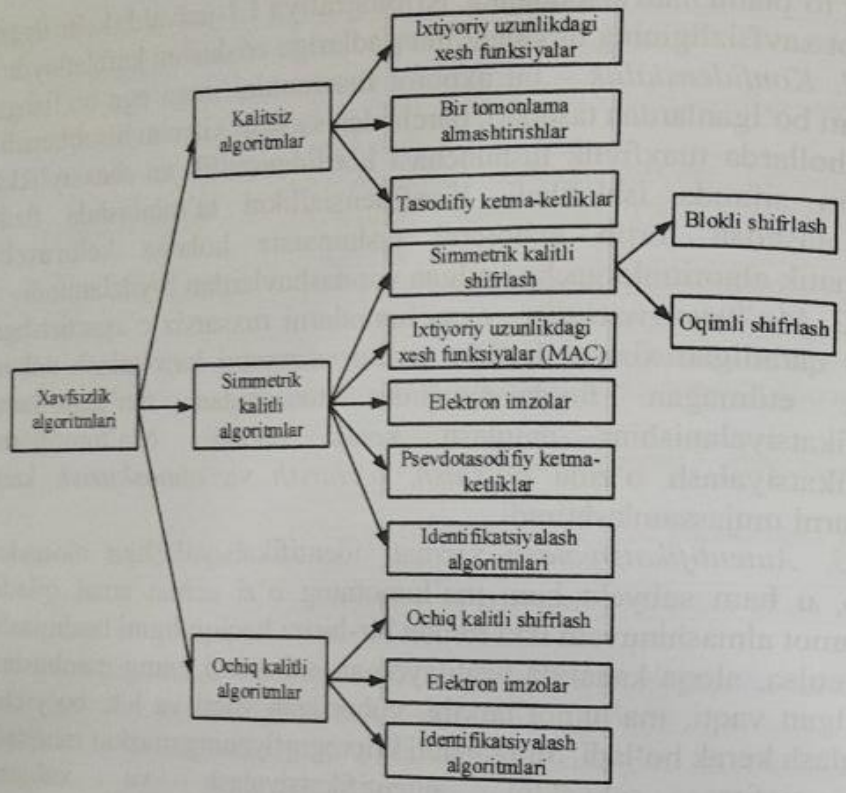
*2. Ma’lumot yaxlitligi* - ma’lumotlarni ruxsatsiz o‘zgartirishga qarshi qaratilgan xizmat bo‘lib, mazkur xizmatni kafolatlash uchun ruxsat etilmagan foydalanuvchilar tomonidan ma’lumotlarni modifikatsiyalanishini aniqlash kerak bo‘ladi. Ma’lumotlarni modifikatsiyalash o‘zida *qo‘shish, o‘chirish* va *almashtirish* kabi amallarni mujassamlashtiradi.

*3. Autentifikatsiyalash* xizmati identifikatsiyalashga aloqador bo‘lib, u ham subyekt ham ma’lumotning o‘zi uchun amal qiladi. Ma’lumot almashinuvchi ikki tomon bir-birini haqiqiyligini tasdiqlashi talab etilsa, aloqa kanalida uzatilayotgan axborotni uning manbasini, yaratilgan vaqti, ma’lumot tarkibi, yuborilgan vaqti va h.k. bo‘yicha tasdiqlash kerak bo‘ladi. Shu sababli kriptografiyaning mazkur maqsadi ikki sinfga: subyektni autentifikatsiyalash va xabarni autentifikatsiyalashga ajratiladi.

*4. Rad eta olmaslik* xizmati avvalgi majburiyatlarni yoki harakatlarni rad etishga to‘sqinlik qiladi. Ko‘p holatlarda subyekt tomonidan muayyan harakatlarni amalga oshirilganligi inkor etilgani bois, nizolar kelib chiqadi. Mazkur muammolarni oldini olishda ishonchli uchinchi tomon ishtirokidagi biror muolaja talab etiladi.

Kriptografiyaning asosiy maqsadi ham nazariyada ham amaliyotda ushbu to‘rtta vazifani yetarli darajada amalga oshirishdan iborat. Shuning uchun kriptografiyani aldash va boshqa zararli harakatlarni aniqlash va ulardan himoyalash haqidagi fan sifatida ham qarash mumkin.

Mazkur o‘quv qo‘llanma axborot xavfsizligini ta’minlashda foydalaniluvchi bir qancha asosiy kriptografik algoritmlarga bag‘ishlangan bo‘lib, 1.1-rasmda ularning umumiy holati aks ettirilgan. Ular haqida ushbu bobda qisqacha to‘xtilib o‘tilsa, keyingi boblarda ular haqida batafsil ma’lumotlar keltiriladi.




*1.1-rasm.* **Kriptografik algoritmlar tasnifi**

Keltirilgan kriptografik algoritmlar quyidagi omillar bo'yicha baholanishi kerak:

*1. Xavfsizlik darajasi.* Ushbu omilni miqdoriy qiymatini aniqlash murakkab bo'lib, qo'yilgan vazifani bajarish uchun zarur bo'lgan amallar soni (joriy vaqtda mavjud bo'lgan eng yaxshi usul va vositalardan foydalangan holda) bo'yicha beriladi.

*2. Funksionallik.* Axborot xavfsizligini turli maqsadlariga erishishda kriptografik algoritmlarni birlashtirish kerak bo'ladi. Berilgan maqsad uchun qaysi kriptografik algoritm eng samarali ekanligi uning xususiyati bilan belgilanadi.

*3. Ishlash usuli.* Kriptografik algoritmlar turli usul va ma'lumotlar bilan qo'llanilganda, turli xususiyatlarni namoyish etadi. Shuning uchun, bitta kriptografik algoritm ishlash uslubi yoki ishlatilishiga qarab turli funksiyalarni taqdim etishi mumkin.



*4. Samaradorlik.* Bu omil ma'lum bir ishlash rejimi uchun kriptografik algoritmning samaradorligini ko'rsatadi (masalan, shifrlash algoritmining darajasi bir sekundda shifrlanuvchi ma'lumot hajmi bilan belgilanishi mumkin).

*5. Amalga oshirishning osonligi.* Bu omil amalda kriptografik algoritmni amalga oshirishning murakkabligini anglatadi. Bu kriptografik algoritmni dasturiy yoki apparat ko'rinishda amalga oshirishning murakkabligini o'z ichiga olishi mumkin.

## 1.2. Kriptografik funksiyalar

Kriptografiya fani matematik bilimlarga asoslangan bo'lib, uning fundamental tushunchalaridan biri – *funksiya* hisoblanadi. Shuningdek, kriptografiyada funksiya tushunchasiga analog bo'lgan *akslantirish* va *almashtirish* tushunchalari ham ishlatiladi.

***Funksiyalar***

To'plam chekli sondagi obyektlardan iborat bo'lib, ular *elementlar* deb ataladi. Masalan, $X$ to'plam $a$, $b$ va $c$ elementlardan iborat bo'lishi mumkin va shuning uchun $X = \{a, b, c\}$ shaklida belgilanadi.

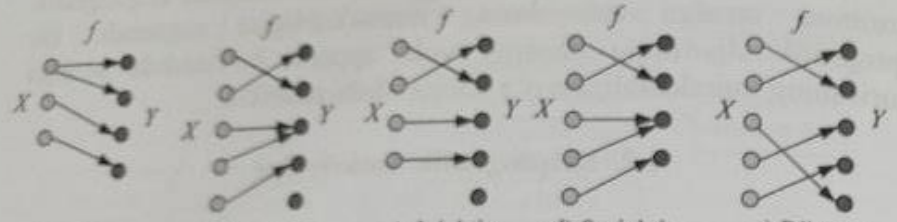
Funksiya ikkita to'plam, $X$ va $Y$ hamda $X$ to'plamdagi har bir elementni $Y$ to'plamdagi bir elementga bog'lovchi $f$ qoida bilan belgilanadi. $X$ to'plam funksiyaning *aniqlanish sohasi* deb atalsa, $Y$ to'plam funksiyaning *qiymatlar sohasi* deb ataladi. Agar $X$ to'plamning elementi $x$ bo'lsa (odatda $x \in X$ shaklida yoziladi) va unga mos qiymatlar sohasining elementi $y$ bo'lsa, uni $y = f(x)$ shaklida ifodalash mumkin. $X$ to'plamdan $Y$ to'plamga akslantiruvchi $f$ funksiyaning standart ifodasi $f: X \to Y$ shaklida ifodalanadi (1.2-rasm "b").

*Ta'rif 1.2.1.* Agar $Y$ qiymatlar sohasining har bir elementi $X$ aniqlanish sohasida eng ko'pi bilan bir elementga mos kelsa, u holda bu funksiya *1-1 (birga bir yoki injektiv) funksiya* deb ataladi (1.2-rasm "c").

*Ta'rif 1.2.2.* Agar $Y$ qiymatlar sohasining har bir elementi $X$ aniqlanish sohasida eng kamida bir elementiga mos kelsa, u holda bu funksiya *ustiga (ko'pga bir* yoki *surjektiv) funksiya* deb ataladi

(1.2-rasm "d"). Agar $f: X \to Y$ funksiya surjektiv bo'lsa, $Im(f) = Y$ shaklida belgilanadi.

*Ta'rif 1.2.3.* Agar $f$ funksiya ham injektiv ham surjektiv bo'lsa, u holda bu funksiya *bijektiv* funksiya deb ataladi (1.2-rasm "d").




a) Funksiya emas | b) Umumiy ko'rinishdagi funksiya | c) Injektiv funksiya (birga-bir) | d) Surjektiv funksiya (ustiga) | e) Bijektiv funksiya (injektiv, surjektiv)

*1.2-rasm.* **Funksiyalarning tasvirlanishi**

*Ta'rif 1.2.4.* Agar $f$ funksiya $X$ to'plamdan $Y$ to'plamga akslantiruvchi bijektiv funksiya bo'lsa, u holda $Y$ to'plamdan $X$ to'plamga akslantiruvchi $g$ bijektiv funksiyani olish mumkin: har bir $y \in Y$ uchun $g(y) = x$ aniqlanadi. Bu yerda, $x \in X$ va $f(x) = y$. Olingan $g$ funksiya $f$ funksiyaning *teskarisi (yoki inversi)* deb ataladi va $g = f^{-1}$ shaklida belgilanadi.

***Bir tomonlama funksiyalar.*** Funksiyalarning shunday turlari mavjudki, ular kriptografiyada muhim o'rin tutadi. Ulardan biri *bir tomonlama* funksiyadir.

*Ta'rif 1.2.5.* Agar $f$ funksiya barcha $x \in X$ uchun oson hisoblanarli, biroq, barcha $y = Im(f)$ lar uchun $f(x) = y$ shartni qanoatlantiruvchi $x \in X$ larni topish imkonsiz bo'lsa, u holda $f$ funksiya $X$ to'plamdan $Y$ to'plamga akslantiruvchi *bir tomonlama funksiya* deb ataladi.

*Misol 1.2.1.* $X = \{1,2,3,\dots,16\}$ va barcha $x \in X$ lar uchun $f(x) = r_x$ o'rinli bo'lsin. Bu yerda, $r_x = 3^x mod 17$ ga teng bo'lsin. U holda funksiya qiymatlari quyidagicha bo'ladi:

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f(x)$ | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |



Yuqorida keltirilgani kabi 1 dan 16 gacha bo'lgan sonlar uchun $f$ funksiya qiymatini hisoblash oson. Biroq, berilgan 7 uchun yuqoridagi jadvaldan foydalanmasdan $f(x) = 7$ shartni qanoatlantiruvchi $x$ elementni topish imkonsiz hisoblanadi.

*Misol 1.2.2.* Tub sonlar birdan katta musbat butun sonlar bo'lib, faqat bir va o'ziga bo'linadi. Tub bo'lgan $p = 48611$ va $q = 53993$ sonlar bo'lsa, u holda $n = p * p = 2624653723$ ga teng. Shuningdek, $X = \{1,2,3,\dots,n-1\}$ ga teng bo'lsin. Aniqlanish sohasi $X$ bo'lgan $f$ funksiya $f(x) = r_x$ ga teng bo'lib, bu yerda $r_x = x^3 mod n$ ga teng. Masalan, $2489991^3 = 5881949859 * n + 1981394214$ bo'lgani bois, $f(2489991) = 1981394214$ ga teng. $f(x)$ funksiyani hisoblash juda oson bo'lib, uning teskarisini aniqlash juda murakkab. Ayniqsa, $n$ noma'lum bo'lganda mazkur muammo yanada murakkablashadi.

***Qopqonli bir tomonlama funksiyalar***

*Ta'rif 1.2.6.* Berilgan ixtiyoriy $y \in Im(f)$ uchun $x \in X$ ni topishda ba'zi ortiqcha axborotni (tuzoqli axborot) taqdim qiluvchi qo'shimcha xususiyatga ega bir tomonlama $f: X \to Y$ funksiyaga qopqonli bir tomonlama funksiya deb ataladi.

1.2.2-misol qopqonli bir tomonlama funksiyani aks ettiradi. Qo'shimcha axborot, $n = 2624653723$ (ya'ni, $p = 48611$ va $q = 53993$, har biri 5 xonali sondan iborat) ma'lum bo'lganda, funksiyani invertini hisoblash oson. 2624653723 sonini hisoblash vositasidan foydalanmasdan faktorlash esa murakkab. Albatta, buni zamonaviy kompyuterlar yordamida osonlik bilan hisoblash mumkin. Boshqa tomondan, $p$ va $q$ sonlari yetarlicha katta tanlansa (masalan, har biri 100 xonadan iborat), hozirgi kundagi hisoblash kompyuterlari yordamida ham ushbu muammoni yechish murakkab hisoblanadi. Ushbu muammo *butun sonni faktorlash* deb nomlanadi.

Bir tomonlama va qopqonli bir tomonlama funksiyalar ochiq kalitli kriptografiyaning asosi hisoblanadi. Ushbu funksiyalarni kriptografik himoyada qo'llanilishini ko'rib chiqqanda ularning ahamiyati yanada aniq bo'ladi.

***O'rin almashtirish funksiyalari***

O'rin almashtirishlar turli kriptografik tuzilmalarda keng qo'llaniluvchi funksiya hisoblanadi.

*Ta'rif 1.2.7.* $S$ chekli sondagi elementlar to'plami berilgan bo'lsin. U holda $p$ *o'rin almashtirish* funksiyasi $S$ to'plamdan o'ziga

akslantiruvchi, $p: S \to S$ (boshqacha aytganda, aniqlanish va qiymatlar sohasi teng) bijektiv funksiyadir.

*Misol 1.2.3.* Faraz qilaylik $S = \{1,2,3,4,5\}$ va o'rin almashtirish funksiyasi $p: S \to S$ quyidagicha bo'lsin:

$$p(1) = 3, p(2) = 5, p(3) = 4, p(4) = 2, p(5) = 1.$$

O'rin almashtirish funksiyasi yuqoridagi kabi yoki quyida keltirilgan massiv kabi akslantirilishi mumkin:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Bu yerda, massivning yuqori qatori o'rin almashtirishning aniqlanishi sohasini ko'rsatsa, pastki qatori qiymatlar sohasini ko'rsatadi.

O'rin almashtirish funksiyasi bijektiv bo'lgani bois, unga teskari bo'lgan funksiya mavjud. Agar o'rin almashtirish funksiyasi $p$ yuqoridagi kabi berilgan bo'lsa, massiv qatorlari o'rnini almashtirish va birinchi qatorni tartiblash orqali $p$ ning teskarisini hosil qilish mumkin:

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}.$$

***Involyutiv funksiyalar***

Kriptografiyada keng qo'llaniluvchi funksiyalardan yana biri *involyutiv* funksiyalar bo'lib, o'zining teskarisiga teng bo'ladi.

*Ta'rif 1.2.8.* Agar $S$ chekli elementdan iborat to'plam va $f$ esa $S$ dan $S$ ga akslantiruvchi bijektiv funksiya bo'lsin. $f = f^{-1}$ shart bo'lsa, $f$ funksiya *involyutiv* deb ataladi. Ushbu tenglikni barcha $x \in S$ lar uchun $f(f(x)) = x$ shaklida ham yozish mumkin.

*Misol 1.2.4.* Faraz qilaylik $S = \{1,2,3,4,5\}$ ga teng bo'lsin. U holda quyidagi $f$ funksiyani $f: S \to S$ involyutiv deb aytish mumkin:

$$f(1) = 4, f(2) = 2, f(3) = 5, f(4) = 1, f(5) = 3.$$



## 1.3. Kriptografiyaning asosiy tushunchalari va atamalari

Har bir fanni o'rganishdan oldin uning asosiy tushunchalarini bilish talab qilinadi. Quyida keyingi bayonlarda ishlatiluvchi asosiy atamalarga oydinlik kiritiladi.

*Alfavit* deganda axborotni ifodalashda ishlatiluvchi belgilarning chekli to'plami tushuniladi. Zamonaviy kriptotizimlarda ko'pincha atigi ikkita simvoldan (0, 1) iborat ikkilik alfavit, A = {0,1}, ishlatiladi. Shuningdek, o'ttiz oltita belgidan (harfdan) iborat o'zbek tili alfavitini, o'ttiz ikkita belgidan (harfdan) iborat rus tili alfavitini, yigirma sakkizta belgidan (harfdan) iborat lotin alfavitini, ikki yuzi ellik oltita belgidan iborat ASCII kompyuter belgilarining alfavitini ham misol sifatida keltirish mumkin.

*Matn* yoki *xabar* – alfavit elementlaridan tartiblangan to'plam. *Ochiq matn* (plaintext, P) – shifrlashga atalgan dastlabki xabar. *Shifrmatn* (cipher text, $C$) – ochiq matnni shifrlash natijasi.

*Kalit* (key, K), yoki kriptoo'zgaruvchi (cryptovariable) – o'zgartirishlar oilasidan birini tanlashni ta'minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati.

*Shifrlash* (encryption, enciphering) – ochiq matnni shifrmatnga o'zgartirish jarayoni, ya'ni, $E_K: P \to C$ kabi belgilanib, u bijektiv funksiya hisoblanadi.

*Rasshifrovkalash* (decryption, deciphering) – shifrmatnni ochiq matnga o'zgartiruvchi teskari jarayon, ya'ni, $D_K: C \to P$ kabi belgilanib, u ham bijektiv funksiya hisoblanadi. Shifrlash va rasshifrovkalash bir – biriga teskari tushunchalar bo'lgani bois, $D_K = E_K^{-1}$ tenglikni yozish mumkin. Shifrlash algoritmi turiga qarab shifrlash va rasshifrovkalash jarayonida foydalanilgan kalitlar o'zaro teng yoki turlicha bo'lishi mumkin.

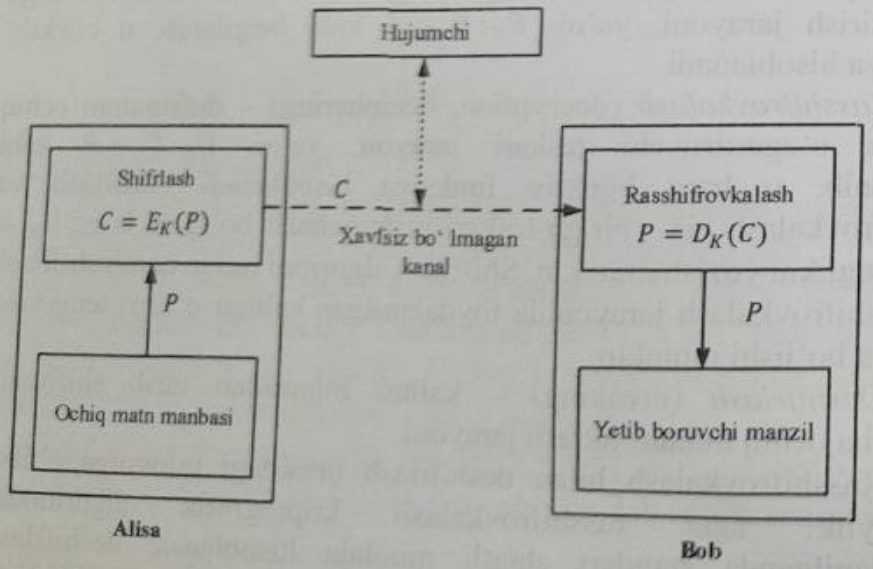
*Deshifrlash* (breaking) – kalitni bilmasdan turib shifrmatn bo'yicha ochiq matnni tiklash jarayoni.

Rasshifrovkalash bilan deshifrlash orasidagi tafovutga e'tibor qarataylik: agar rasshifrovkalash kriptografik algoritmdan foydalanilganda standart shtatli muolaja hisoblansa, deshifrlash, ko'proq kriptotahlilga taalluqli, kriptotizimni buzishdir. "Shifrlash" umumiy atamasi shifrlash va rasshifrovkalash jarayonini bildiradi.

Shifrlash jarayonidan axborotni konfidensialligini ta'minlash maqsadida foydalanilish mumkin. Ikki tomon, Alisa va Bob, o'rtasida dastlab kalit $K$ (faraz qilinsin, shifrlash va rasshifrovkalash uchun bir xil kalitdan foydalanilgan bo'lsin) maxfiy tarzda yetkazilgan bo'lsin. Agar Alisa $P$ ochiq matnni yubormoqchi bo'lsa, u holda $C = E_K(P)$ qiymatni hisoblaydi va Bobga yuboradi. Bob $C$ ni qabul qilishi bilan $P = D_K(C)$ ni hisoblaydi va haqiqiy ochiq matn $P$ ni tiklaydi.

Shifrlash va rasshifrovkalash jarayonida kalitdan foydalanilganiga e'tibor qarataylik. Nima uchun shunchaki biror shifrlash funksiyasi va unga mos rasshifrovkalash funksiyasidan foydalanish mumkin emas? Shifrlash va rasshifrovkalash funksiyasida kalitdan foydalanishdan asosiy maqsad har bir ma'lumot uchun ularni qayta loyihalashdan qochishdir. Ya'ni, faqat shifrlash va unga mos rasshifrovkalash funksiyasidan foydalanilganda agar buzg'unchi ularni aniqlasa, yangi shifrlash/ rasshifrovkalash funksiyasini loyihalash talab etiladi. Agar kalitdan foylanilgan bo'lsa, unda faqat kalitni almashtirishning o'zi yetarli bo'ladi.

Umumiy holda shifrlashga asoslangan ikki tomon orasida tashkil qilingan aloqaning umumiy ko'rinishi 1.3-rasmda keltirilgan.




*1.3-rasm.* **Shifrlashga asoslangan ikki tomon o'rtasida tashkil etilgan aloqa sxemasi**



Yuqorida keltirilgan shifrlashga asoslangan aloqa sxemasida quyidagi ishtirokchilar mavjud:

- *subyekt* yoki *tomon* axborotni jo'natuvchi, qabul qiluvchi va o'zgartiruvchi foydalanuvchi yoki uning nomidan ishlovchi elektron qurilma. 1.3-rasmdagi Alisa va Bob keltirilgan aloqa sxemasi uchun subyekt sifatida xizmat qiladi. Subyekt sifatida shaxs, hisoblash mashinasi va h.k. xizmat qilishi mumkin.
- *jo'natuvchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida axborotni qonuniy uzatuvchi subyekt hisoblanib, 1.3-rasmda Alisa sifatida aks ettirilgan.
- *qabul qiluvchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida axborotni qonuniy qabul qiluvchi subyekt hisoblanib, 1.3-rasmda Bob sifatida aks ettirilgan.
- *hujumchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida jo'natuvchi ham, qabul qiluvchi ham bo'lmagan, biroq, jo'natuvchi va qabul qiluvchi o'rtasida ta'minlangan axborot xavfsizligini buzishga harakat qiluvchi ikki tomonlama aloqada bo'lgan subyekt. Ushbu subyektning hujumchidan tashqari ko'plab nomlari, xakker, buzg'unchi, g'araz niyatli va h.k. mavjud. Ikki tomon o'rtasida tashkil qilingan aloqa sxemasida hujumchi ham jo'natuvchi ham qabul qiluvchi rolida bo'lishi mumkin.

Bundan tashqari, tomonlar o'rtasida o'rnatilgan aloqa kanali ham kriptografiyada muhim ahamiyatga ega. Aloqa kanallariga oid quyidagi tushunchalar mavjud:

- *kanal* – axborotni boshqa tomonga yetkazish vositasi;
- *fizik xavfsiz kanal* yoki *xavfsiz kanal* – hujumchi fizik kira olmaydigan kanal;
- *himoyalanmagan kanal* – axborot nisbatan qonuniy foydalanish huquqiga ega tomonlardan tashqari tomonlar ham axborotni o'zgartirishi, o'qishi, o'chirishi va kiritishi mumkin bo'lgan kanal;
- *himoyalangan kanal* – hujumchiga axborotni o'zgartirish, o'qish, o'chirish va kiritish imkoniyatini taqdim etmagan kanal.

Kriptotizimni ikki tarkibli algoritm va kalitdan iborat ekanligiga asoslangan holda *Kerkgoff prinsipini* eslatib o'tish lozim. Ushbu prinsipga binoan faqat kalit sir saqlanishi, shifrlash algoritmi esa ochiq bo'lishi lozim. Bu degani, agar niyati buzuq algoritmni bilgan taqdirda

ham tizim obro'sizlanmaydi. Kalitni esa almashtirish mumkin. Klod Shennon ushbu prinsipni "Dushman tizimni biladi", deb ta'riflagan.

*Ta'rif 1.3.1.* Belgilangan vaqt ichida hujumchi rasshifrovkalash kalitini bilmasdan shifrmatndan ochiq matnni tiklay olmasa bunday shifrlash sxemasi *bardoshli* deb aytiladi.

Kriptotizimlarni buzish usullari *kriptotahlil* (cryptoanalysis)ni o'rganish predmeti hisoblanadi. Kriptografiya va kriptotahlil uzviy bog'langanliklari sababli, ularni ko'pincha birgalikda yagona fan – *kriptologiya* (cryptology) (*kryptos* - mahfiy, *logos*- ilm) sifatida qabul qilinadi.

*Kriptotizim* (cryptosystem) – ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifrmatnga qaytariluvchan o'zgartirishlar oilasi.

Kriptografik usullar umumiy xususiyatlari bo'yicha ikki turga, *simmetrik* va *ochiq kalitli*ga bo'linadi. Ular bilan keyingi bo'limlarda tanishib chiqiladi.

### 1.4. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalar

Ushbu bo'limda simmetrik kalitli shifrlash algoritmlari va xesh funksiyalarga oid umumiy ma'lumotlar bilan tanishib chiqiladi.

*Ta'rif 1.4.1.* Ma'lumotni shifrlash va rasshifrovkalash uchun yagona kalitdan foydalanuvchi shifrlash – *simmetrik kalitli shifrlash* usuli (ba'zi adabiyotlarda *yagona kalitli, bir kalitli, shaxsiy kalitli shifrlash* deb ham yuritiladi) deb aytiladi.

*Misol 1.4.1.* Faraz qilaylik $A = \{a, b, c, \dots, x, y, z\}$ Ingliz harflaridan iborat alfavit bo'lsin. Kalit $K$ sifatida esa $A$ alfavitni almashtirish (har bir elementini o'ngga siljitish) soni qaralsin va $K =$ 3 ga teng bo'lsin. U holda yangi alfavitni $B = \{d, e, f, \dots, a, b, c\}$ga engligini bilish oson. Umumiy holda ikki alfavit quyidagiga teng o'ladi:

| | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| = | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |

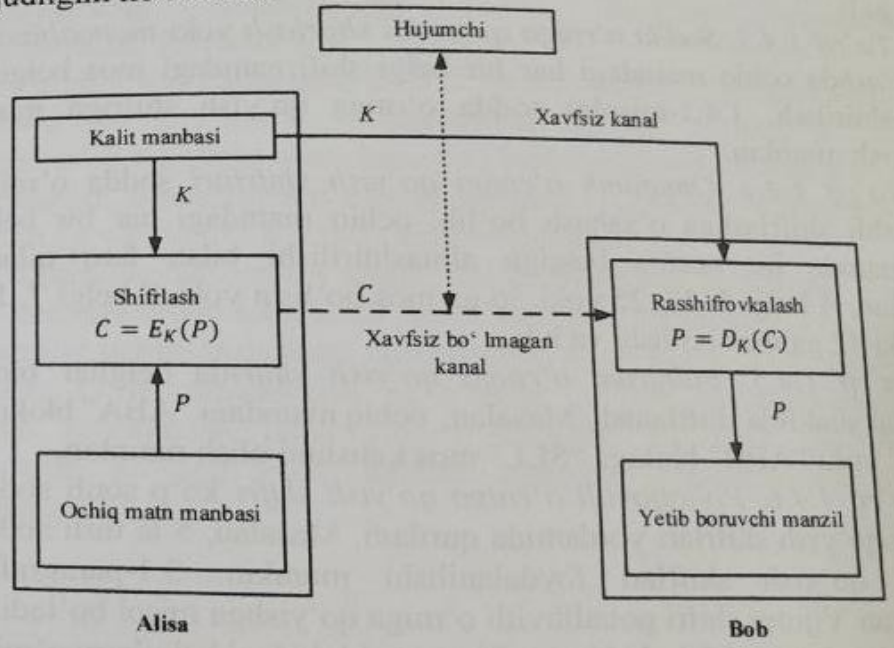
Shifrlash usuli sifatida esa ochiq matn belgilarini $A$ alfavitdan b, unga mos shifrmatn belgisini $B$ alfavitdan topish qaralgan sin. Agar ochiq matn $P =$ "*bu sodda shifrlash usuli*" ga teng



bo'lsa, u holda shifrmatn $C =$ "*ex vrggd vkliuodvk xvxol*" ga tengligini bilish oson.

Rasshifrovkalashda shifrmatn belgilari $B$ alfavitdan olinib, unga mos ochiq matn belgilari $A$ alfavitdan olinadi. Keltirilgan misolda kalit sifatida ochiq matn belgilari olingan $A$ alfavitdan mos bo'lgan shifrmatn belgilari olinuvchi $B$ alfavitni hosil qiluvchi o'ngga siljitishlar soni olingan.

Umumiy holda ikki tomon o'rtasida simmetrik kalitli shifrlashdan foydalanib tashkil qilingan aloqa sxemasini quyidagicha tasvirlash mumkin (1.4-rasm). Ko'rish mumkinki, ma'lumotni shifrlash kalitini Bobga yetkazish uchun xavfsiz aloqa kanali talab qilinmoqda. Bu esa, simmetrik kalitli shifrlarda *kalitlarni xavfsiz taqsimlash* muammosi mavjudligini ko'rsatadi.




*1.4-rasm.* **Simmetrik kalitli shifrlashga asoslangan ikki tomon o'rtasidagi aloqa sxemasi**

Simmetrik kalitli shifrlash sxemalari ikkita sinfga: *blokli shifrlar* va *oqimli shifrlar*ga ajratiladi.

*Ta'rif 1.4.2. Blokli shifrlar* $A$ alfavitda ochiq matnni o'zgarmas $t$ uzunlikdagi qismlarga (*bloklar* deb ataladi) bo'luvchi shifrlash sxemasi bo'lib, bir vaqtning o'zida bitta blokni shifrlaydi.

Blokli shifrlar keng tarqalgan shifrlash sxemalaridan bo'lib, uning *o'rniga qo'yishga asoslangan* va *o'rin almashtirishga asoslangan* ikki muhim sinfi mavjud.

***O'rniga qo'yish***ga asoslangan shifrlarda ochiq matn belgilarining o'rniga boshqa belgilar yoki belgilar guruhini qo'yish bilan shifrmatn hosil qilinadi. Qabul qiluvchi esa rasshifrovkalash uchun teskari o'rniga qo'yishni amalga oshirish bilan haqiqiy matnni tiklaydi.

An'anaviy kriptografiyada o'rniga qo'yish shifrlarining to'rt turi mavjud:

*Ta'rif 1.4.3. Sodda o'rniga qo'yishli shifrlash* yoki *monoalfavitli shifrlash*da ochiq matndagi har bir belgi shifrmatndagi mos belgiga almashtiriladi. 1.4.1-misolni sodda o'rniga qo'yish shifriga misol keltirish mumkin.

*Ta'rif 1.4.4. Omofonik o'rniga qo'yish shifrlari* sodda o'rniga qo'yishli shifrlashga o'xshash bo'lib, ochiq matndagi har bir belgi shifrmatnda bir nechta belgiga almashtirilishi bilan farq qiladi. Masalan, $A$ belgi 5, 13, 25 yoki 56 ga mos bo'lishi yoki $B$ belgi 7, 19, 31 yoki 42 ga mos bo'lishi va h.k.

*Ta'rif 1.4.5. Poligram o'rniga qo'yish shifri*da belgilar bloki guruhlar shaklida shifrlanadi. Masalan, ochiq matndagi "ABA" blokiga "RTQ" yoki "ABB" blokiga "SLL" mos kelishini olish mumkin.

*Ta'rif 1.4.6. Polialfavitli o'rniga qo'yish shifri* ko'p sonli sodda o'rniga qo'yish shifrlari yordamida quriladi. Masalan, 5 ta turli sodda o'rniga qo'yish shifrlari foydalanilishi mumkin. 3.1-paragrafda keltirilgan Vijiner shifri polialfavitli o'rniga qo'yishga misol bo'ladi.

***O'rin almashtirish*** shifrlari ochiq matn blokidagi belgilarni o'rnini almashtirishga asoslanadi. Boshqacha aytganda, ochiq matndagi belgilarning tarkibi o'zgarmas saqlanib, tartibi o'zgaradi. Bunga ochiq matnni jadvalga ustun bo'yicha yozib, satr bo'yicha o'qib olishni misol keltirish mumkin.

*Misol 1.4.2.*

*Ochiq matn:* "sodda_o'rin_almashtirish_funksiyasi"



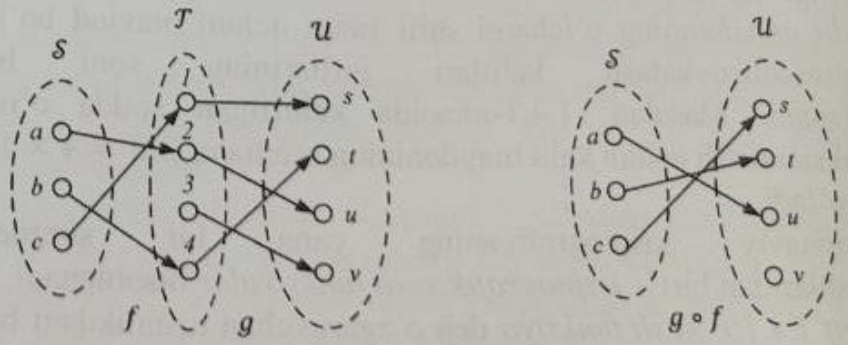
| | | | |
|---|---|---|---|
| s | i | t | n |
| o | n | i | k |
| d | _ | r | s |
| d | a | i | i |
| a | l | sh | y |
| _ | m | _ | a |
| o' | a | f | s |
| r | sh | u | i |

*Shifr matn:* "sitnonikd_rsdaiialshy_m_ao'afsrshui".

Hozirda zamonaviy shifrlarni qurishda bir qancha sodda funksiyalarning majmuasidan iborat bo'lgan *funksiyalar birlashmasi*dan foydalaniladi.

*Ta'rif 1.4.7.* Faraz qilaylik $S, T$ va $U$ – chekli to'plamlar hamda $f: S \to T$ va $g: T \to U$ – funksiyalar bo'lsin. $f$ ning $g$ bilan birlashmasi $g \circ f$ (yoki shunchaki $fg$) kabi belgilanib, funksiya $S$ dan $U$ to'plamga almashtirishni amalga oshiradi (1.5-rasm) va barcha $x \in S$ uchun $(g \circ f)(x) = g(f(x))$ kabi belgilanadi.

Keltirilgandan xulosa qilgan holda, birlashma funksiyani 2 dan ortiq funksiyalardan ham hosil qilish mumkin. Masalan, $f_1, f_2, \ldots, f_t$ funksiyalar uchun birlashma funksiyani $f_t \circ \ldots \circ f_2 \circ f_1$ kabi ifodalash mumkin. O'rin almashtirish va o'rniga qo'yish akslantirishlaridan alohida foydalanish bilan yuqori bardoshli shifrlarni qurishning imkoniyati yo'qligi bois, amalda ularning birlashmasidan keng foydalaniladi.




***1.5-rasm.*** ***g* va *f* funksiyalarning $g \circ f$ birlashmasi**

Simmetrik kalitli shifrlarning yana bir keng tarqalgan ko'rinishi bu – *oqimli shifrlar*. Tarmoq bo'ylab uzatiladigan axborot tashqi xalallar tufayli o'zgarishi kuzatiladigan muhitlarda oqimli shifrlardan keng foydalaniladi.

*Ta'rif 1.4.8.* Faraz qilaylik $\mathcal{K}$ shifrlash akslantirishlari to'plami uchun kalit maydoni bo'lsin. U holda, $e_1e_2e_3\cdots e_i \in \mathcal{K}$ belgilar ketmaketligi *kalit oqimi* deb ataladi.

*Ta'rif 1.4.9.* Faraz qilaylik $\mathcal{A}$ alfavit $q$ belgidan iborat va $e \in \mathcal{K}$ uchun $E_e$ blok uzunligi birga teng bo'lgan sodda o'rniga qo'yish shifri bo'lsin. Shuningdek, ochiq matn qatori $m_1m_2m_3\cdots$ va $\mathcal{K}$ dan olingan kalit oqimi $e_1e_2e_3\cdots$ ga teng bo'lsin. U holda *oqimli shifr* ochiq matn qatorini qabul qilib, shifrmatn qatori $c_1c_2c_3\cdots$ ni $c_i = E_{e_i}(m_i)$ tenglik orqali hosil qilinadi. Agar $d_i$ qiymat $e_i$ ning teskarisi bo'lsa, u holda ochiq matn $D_{d_i}(c_i) = m_i$ ga ega bo'linadi.

Oqimli shifrlarda foydalanilgan kalit oqimiga asoslangan holda sodda akslantirishlar qo'llaniladi. Kalit oqimi tasodifiy tarzda yoki kichik uzunlikdagi boshlang'ich kalitdan *kalit oqimi generatori* deb nomlanuvchi biror algoritm asosida hosil qilinadi.

*Misol 1.4.3. Vernam shifri* $\mathcal{A} = \{0,1\}$ alfavit uchun aniqlangan oqimli shifr hisoblanadi. $t$ bit uzunlikdagi binar xabar $m_1m_2m_3\cdots m_t$ uzunligiga teng bo'lgan binar kalit $k_1k_2k_3\cdots k_t$ bilan XOR amalida $c_1c_2c_3\cdots c_t$ shifrmatnni hosil qiladi:

$$c_i = m_i \oplus k_i,\ 1 \le i \le t.$$

Agar kalit qatori tasodifiy tanlansa va takrorlanmasa, Vernam shifri *bir martali tizim* yoki *bir martali bloknot* deb ataladi.

*Kalit maydonining* o'lchami shifr tizim uchun mavjud bo'lgan shifrlash/rasshifrovkalash kalitlari juftlarining soni bilan arakterlanadi. Masalan, 1.4.1-misolda keltirilgan sodda o'rniga o'yish akslantirish uchun kalit maydonining o'lchami $26! \approx 4 \times 10^{26}$ teng bo'ladi.

Zamonaviy kriptografiyaning yana bir simmetrik lantirishlaridan biri – *kriptografik xesh funksiyalar* hisoblanadi.

*Ta'rif 1.4.10. Xesh funksiya* deb o'zgaruvchan uzunlikdagi binar rlarni *xesh qiymat* deb ataluvchi biror o'zgarmas uzunlikdagi



qiymatga samarali hisoblashlar orqali aks ettiruvchi bir tomonlama funksiyaga aytiladi.

$n$ bitli xesh qiymatlarni (masalan, $n = 128$ yoki 160) qaytaruvchi va talab etilgan xususiyatlarga ega xesh funksiya uchun tasodifiy kiruvchi satrning ma'lum bir xesh qiymatga bog'lanish ehtimoli $2^{-n}$ ga teng bo'ladi. Buning uchun, biror $h$ kriptografik xesh funksiyani loyihalashda ikkita turli kirish qiymatlari uchun bir xil xesh qiymatni hosil bo'lishini imkonsizligiga e'tibor qaratiladi (ya'ni, $x \neq y$ kiruvchi qatorlar uchun $h(x) = h(y)$ holat kuzatilmasligi shart).

Kriptografik xesh funksiyalar axborot xavfsizligida elektron raqamli imzo algoritmlarini yaratishda va ma'lumotlar yaxlitligini ta'minlashda foydalaniladi.

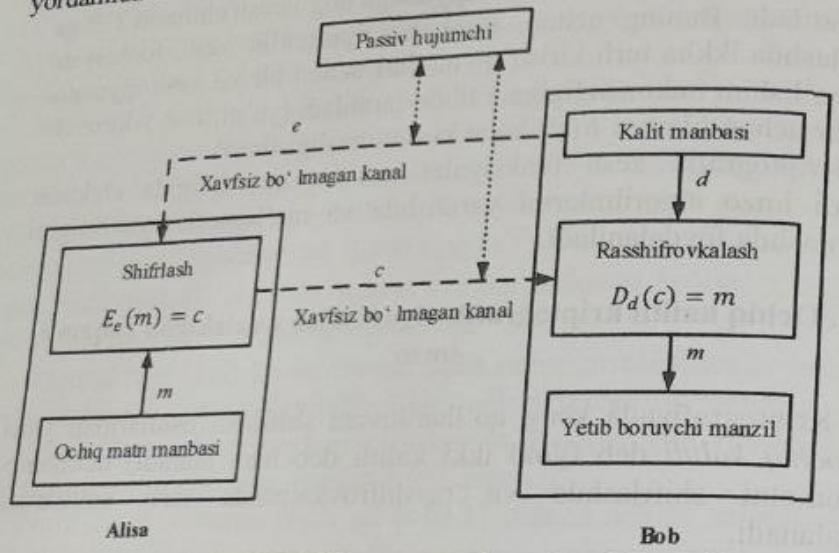
## 1.5. Ochiq kalitli kriptografik algoritmlar va elektron raqamli imzo

Kriptografiyada keng qo'llaniluvchi shifrlash usullaridan yana biri *ochiq kalitli* deb (yoki ikki kalitli deb ham ataladi) nomlanib, ma'lumotni shifrlashda va rasshifrovkalashda turli kalitlardan foydalanadi.

Faraz qilaylik, $\mathcal{K}$ kalit maydonida $\{E_e : e \in \mathcal{K}\}$ shifrlash funksiyasi va $\{D_d : d \in \mathcal{K}\}$ unga mos rasshifrovkalash funksiyasi bo'lsin. Shuningdek, barcha shifrlash/rasshifrovkalash funksiyalari jufti $(E_e, D_d)$ uchun berilgan shifrmatn $c \in C$ uchun $E_e$ funksiya yordamida ochiq matn $m \in M$ ni $(E_e(m) = c$ shartni qanoatlantiruvchi) hisoblashning imkoni mavjud bo'lmasin. Bu xususiyat, berilgan shifrlash kaliti $e$ dan foydalanib, rasshifrovkalash kaliti $d$ ni topishning imkonsizligini ko'rsatadi. Bu yerda, $E_e$ – qopqonli bir tomonlama funksiya hisoblanib, uni teskarisini topish uchun faqat $d$ parametr talab etiladi. Shu sababli, ochiq kalitli shifrlash algoritmlari shifrlash va rasshifrovkalash kalitlari bir xil bo'lgan, simmetrik shifrlardan farqlanadi.

Ochiq kalitli shifrlash algoritmi yordamida hosil qilingan ikki tomon o'rtasidagi aloqa kanalining umumiy ko'rinishi 1.6-rasmda keltirilgan. Bunga ko'ra, Bob $(e, d)$ kalit juftlarini tanlaydi. Shifrlash kaliti $e$ (*ochiq kalit* deb ataladi)ni Alisaga ochiq tarmoq orqali yuboradi va rasshifrovkalash kaliti $d$ (*shaxsiy kalit* deb ataladi)ni o'zida maxfiy

saqlaydi. Shundan so'ng, Alisa ochiq matn $m$ ni Bobning ochiq kaliti yordamida shifrlaydi: $c = E_e(m)$ va uni ochiq tarmoq orqali yuboradi. Bob esa qabul qilingan shifrmatn $c$ ni $d$ kalit bilan $D_d$ funksiya yordamida rasshifrovkalaydi.



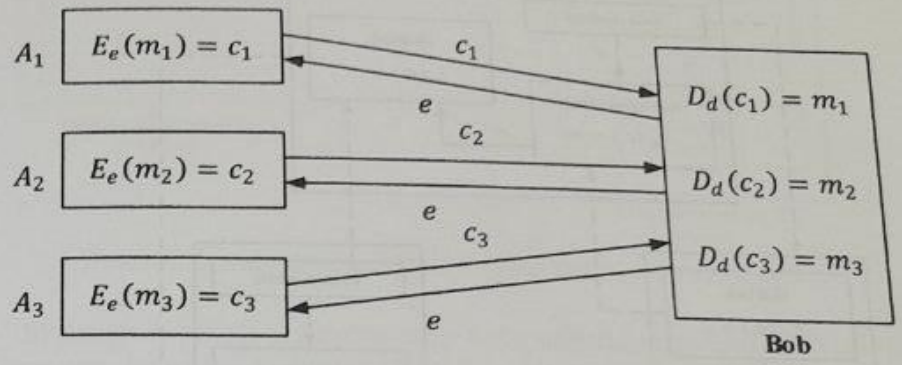

*1.6-rasm.* **Ochiq kalitli shifrlash usuli yordamida shifrlash**

Ochiq kalitli shifrlash algoritmlari yordamida shifrlash jarayoni shifrlash kalitini ochiq yuborilishi bilan simmetrik kalitli shifrlardan farq qiladi. Bundan tashqari, ochiq kalitli shifrlash algoritmlari yordamida ma'lumot uzatishda simmetrik kriptotizimlar kabi har bir ma'lumot uzatuvchi va qabul qiluvchi orasida alohida – alohida kalitdan foydalanishni talab etmaydi. Bobning ochiq kaliti $e$ ni bilgan har bir ishtirokchi ma'lumotni shifrlab unga yuborishi mumkin. Shifrlangan ma'lumotni rasshifrovkalash esa faqat $d$ kalitni bilgan Bob uchun joiz bo'ladi. Mazkur holat 1.7-rasmda keltirilgan. Bu yerda $A_1$, $A_2$ va $A_3$ turli tomonlar bo'lib, Bobning yagona kaliti $e$ bilan $m_1$, $m_2$ va $m_3$ ma'lumotlarni shifrlashi mumkin bo'ladi. Hosil bo'lgan barcha shifrmatnlarni esa Bob yagona shaxsiy kalit $d$ bilan rasshifrovkalashi mumkin bo'ladi.

Ochiq kalitli shifrlash algoritmlari shifrlash kalitini uzatish uchun xavfsiz kanalni talab etmasligi bilan ajralib tursada, bu amalda to'liq



xavfsizlikni ta'minlash uchun yetarli hisoblanmaydi. 1.8-rasmda buzg'unchi tomonidan ochiq kalitli shifrlash algoritmini buzmasdan ma'lumotni qo'lga kiritish jarayoni keltirilgan. Mazkur holat *obro'sizlantirish* deb ataladi.




*1.7-rasm.* **Ochiq kalitli shifrlashdan foydalanish sxemasi**

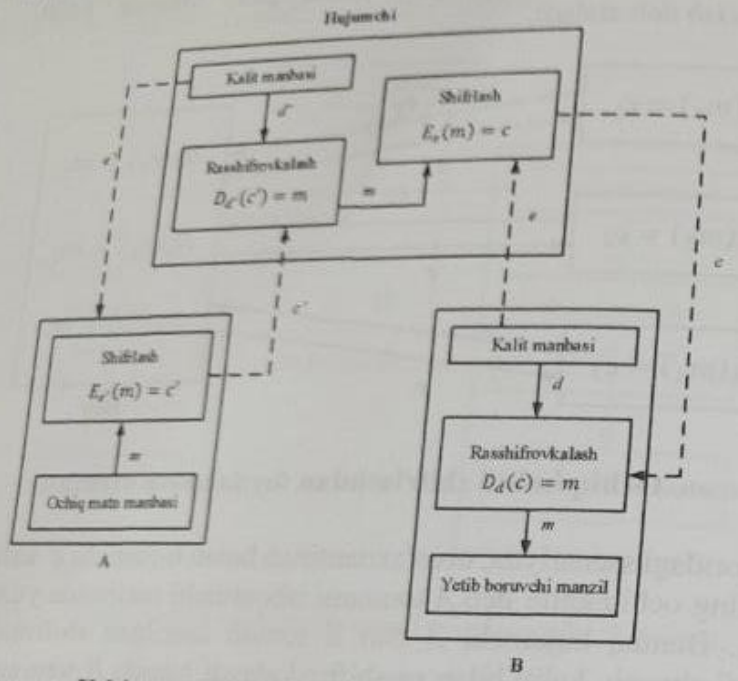
Yuqoridagi ssenariyda, obro'sizlantirish holati hujumchi $e'$ kalitni $B$ tomonning ochiq kaliti deb $A$ tomonni ishontirishi natijasida yuzaga kelmoqda. Bunda, hujumchi $A$ dan $B$ tomon uzatilgan shifrmatnni o'zining $d'$ shaxsiy kaliti bilan rasshifrovkalaydi hamda $B$ tomonning ochiq kaliti $e$ bilan qayta shifrlab unga yuboradi. Mazkur holda muammo $A$ tomon ochiq kalitni $B$ tomonga tegishli ekanligini tekshira olmasligi natijasida yuzaga kelmoqda.

Amalda ochiq kalitli shifrlash algoritmlaridan elektron raqamli imzo deb ataluvchi tizimni qurish uchun foydalaniladi. Elektron raqamli imzo algoritmlari ochiq kalitli kriptotizimlarning bir turi hisoblanadi. Faraz qilaylik, $E_e$ ochiq matn maydoni $\mathcal{M}$ dan shifrmatn maydoni $\mathcal{C}$ ga akslantiruvchi shifrlash funksiyasi va bunda $\mathcal{M} = \mathcal{C}$ bo'lsin. Agar $E_e$ ga mos bo'lgan rasshifrovkalash funksiyasi $D_d$ bo'lsa, u holda $E_e$ va $D_d$ lar uchun o'rin almashtirish mumkin:

$$\text{barcha } m \in \mathcal{M} \text{ lar uchun, } D_d\big(E_e(m)\big) = E_e\big(D_d(m)\big) = m.$$

Ochiq kalitli shifrlashning mazkur ko'rinishi *qaytariladigan* deb ataladi. Bunda, faqat $m \in \mathcal{M}$ holat uchun $\mathcal{M} = \mathcal{C}$ o'rinli bo'lishini

inobatga olish kerak. Qolgan holatlarda esa $(m \notin C)$, $D_d(m)$ akslantirish ma'noga ega bo'lmaydi.




*1.8-rasm.* **Ikki tomon orasidagi aloqaning obro'sizlantirilishi**

Elektron raqamli imzo tizimlarini qurish quyidagi tartibda amalga oshiriladi (1.9-rasm):

1. Faraz qilaylik imzolash sxemasi uchun $\mathcal{M}$ ochiq matn maydoni bo'lsin.

2. Faraz qilaylik imzo maydoni $\mathcal{S}$ uchun $\mathcal{M} = C$ o'rinli bo'lsin.

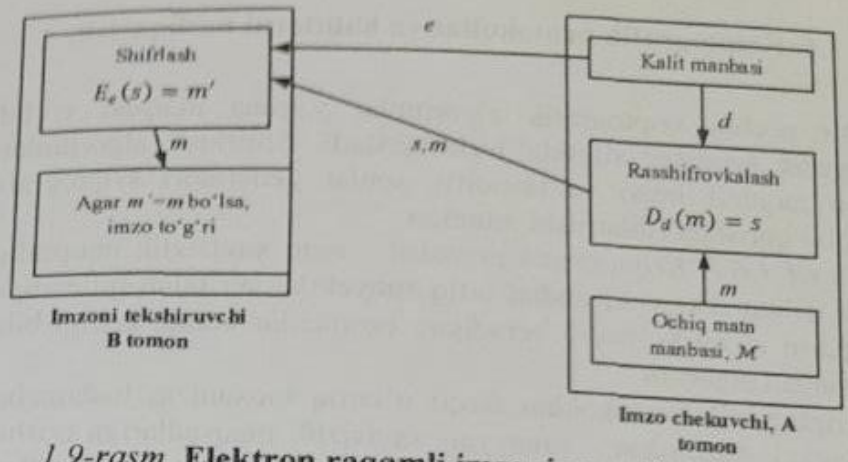
3. Faraz qilaylik $(e, d)$ – ochiq kalitli shifrlash sxemasi uchun kalit juftli bo'lsin.

4. Imzolash funksiyasi $S_A$ ni $D_d$ ga teng deb olsak, u holda $m \in$ xabarlar uchun imzo $s = D_d(m)$ ga teng bo'ladi.

5. Imzoni tekshirish funksiyasi $V_A$ esa quyidagiga teng bo'ladi:

$$V_A(m,s) = \begin{cases} true, & agar\ E_e(s) = m \\ false, & qolgan\ hollarda. \end{cases}$$






*1.9-rasm.* **Elektron raqamli imzoning sodda sxemasi**

Simmetrik kalitli kriptotizimlar kabi ochiq kalitli shifrlash orqali ma'lumotni konfidensialligini ta'minlash amalga oshiriladi. Biroq, elektron raqamli imzo tizimlari ma'lumotni yaxlitligini va rad etishdan himoyasini ta'minlashni maqsad qiladi.

Yuqorida ko'rib o'tilgan simmetrik va ochiq kalitli kriptotizimlar o'ziga xos qator afzallik va kamchiliklarga ega. Xususan, ularga quyidagilarni keltirish mumkin (1.2-jadval).

*1.2-jadval*

**Simmetrik va ochiq kalitli kriptotizimlarning afzalliklari va kamchiliklari**

| Xususiyat / Kriptotizim | Afzallik | Kamchilik |
|---|---|---|
| **Simmetrik kriptotizimlar** | 1. Simmetrik kalitli shifrlar ma'lumotni shifrlashda yuqori tezkorlik taqdim etadi.<br>2. Simmetrik kriptotizim kalitining uzunligi nisbatan qisqa. | 1. Simmetrik kriptotizimdan foydalanish uchun ikki tomonda ham yagona kalit bo'lishi shart.<br>2. Simmetrik kalitlardan foydalanish davri kam. |
| **Ochiq kalitli kriptotizimlar** | 1. Faqat shaxsiy kalitni maxfiy saqlash talab etiladi.<br>2. Shaxsiy va ochiq kalitlar juftida yetarlicha uzoq vaqt foydalanish mumkin. | 1. Ochiq kalitli shifrlar ma'lumotlarni shifrlashda past tezkorlik qayd etadi.<br>2. Ochiq kalitli kriptotizimlarda kalit uzunligi nisbatan katta. |

Bir nechta kriptografik algoritmlar yagona maqsad yo'lida *kriptografik protokol* sifatida birlashtiriladi. Shifrlash algoritmlari, elektron raqamli imzo va tasodifiy sonlar generatori kriptografik protokolni qurishda ishlatilishi mumkin.

*Ta'rif 1.6.1. Kriptografik protokol* – aniq xavfsizlik maqsadiga erishish uchun ikki yoki undan ortiq subyektlardan talab qilinadigan harakatlarni izchil ko'rsatib beradigan bosqichlar ketma-ketligi bilan taqsimlangan algoritm.

Kriptografik protokoldan farqli o'laroq mexanizm tushunchasi ham mavjud. *Mexanizm* – muayyan xavfsizlik maqsadlariga erishish uchun protokollarni, algoritmlarni va kriptografik bo'lmagan usullarni o'z ichiga olgan umumiy atama.

*Misol 1.6.1. (Sodda kalit almashinish protokoli).* Alisa va Bob xavfsiz bo'lmagan kanal orqali aloqa o'rnatish uchun simmetrik shifrlash tizimini tanladilar. Bu o'rinda, ma'lumotni shifrlash uchun ularga kalit zarur bo'ladi. Mazkur holda tomonlar o'rtasida aloqa o'rnatish protokoli quyidagicha bo'ladi:

1. Bob ochiq kalitni shifrlash algoritmini tanlaydi va o'zining ochiq kalitini kanal orqali Alisaga yuboradi.
2. Alisa ma'lumotlarni shifrlash uchun simmetrik kriptotizim kalitini generatsiya qiladi.
3. Alisa simmetrik kriptotizim kalitini Bobning ochiq kaliti bilan shifrlagan holda uni Bobga yuboradi.
4. Bob o'zining shaxsiy kaliti yordamida simmetrik kriptotizim kalitini qayta tiklaydi.
5. Shundan so'ng, Alisa va Bob umumiy simmetrik kalitga va uning yordamida ma'lumotlarni shifrlab uzatish imkoniyatiga ega bo'ladilar.

Mazkur protokolning maqsadi xavfsiz bo'lmagan tarmoqda xavfsiz aloqani qurish hisoblanadi va buning uchun ochiq kalitli va simmetrik shifrlash tizimlaridan foydalanilgan.

Amalda kriptografik funksiyalar alohida-alohida tarzda emas, balki kriptografik protokol sifatida keng qo'llaniladi. Bu esa qurilayotgan kriptografik protokolning xavfsizligi nafaqat unda



foydalanilgan algoritmlarga, shuningdek, ularning birgalikda qanday loyihalanganligiga ham bog'liq bo'ladi.

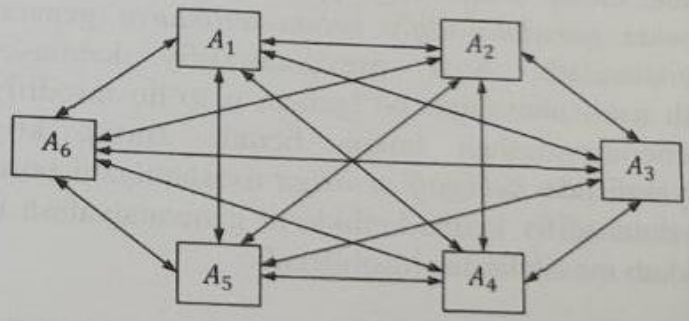
Yuqorida simmetrik, ochiq kalitli va elektron raqamli imzo kabi kriptotizimlar bilan tanishib o'tildi. Xususan, ularning har biri uchun kalitlarni generatsiyalash jarayoni mavjudligini ko'rishimiz mumkin. Kriptografik kalitlarni generatsiyalash va kalitni o'rnatish kabi vazifalar bilan kriptografiyaning *kalitlarni boshqarish* deb nomlangan bo'limi shug'ullanadi.

*Ta'rif 1.6.2. Kalitni o'rnatish* – ikki yoki undan ortiq tomonlarga keyingi kriptografik algoritmlar foydalanishi uchun kerak bo'lgan kalitni taqsimlash jarayoni.

*Ta'rif 1.6.3. Kalitni boshqarish* – kalitlarni o'rnatishni madadlovchi, tomonlar o'rtasida doimiy aloqani saqlab turuvchi hamda kalitlar eskirganda ularni yangilovchi jarayon va mexanizmlarning to'plami.

Kalitlarni o'rnatish jarayoni o'zida *kalitlarni kelishish* va *kalitlarni uzatish* qism jarayonlarini mujassamlashtirgan. Kalitlarni o'rnatish jarayoni ko'plab protokollar tomonidan amalga oshirilgan.

Kalitlarni o'rnatish simmetrik kriptotizimlar uchun jiddiy muammolardan hisoblanadi. Xususan, 6 ta ishtirokchi o'rtasida kalitni o'rnatish holatining ko'rinishi 1.10-rasmda keltirilgan.




*1.10-rasm.* **Olti tomon o'rtasidagi kalitlarning bog'lanishi**

Ma'lumot almashmoqchi bo'lgan har bir tomon o'rtasida alohida-alohida simmetrik kalitlar talab qilingani bois, tomonlar o'rtasidagi jami simmetrik kalitlar soni $\binom{n}{2} = \frac{n(n-1)}{2}$ tenglik bilan aniqlanadi. Bu

yerda, $n$ – tomonlar soni bo'lib, 6 ta tomon uchun umumiy simmetrik kalitlar soni 15 ga teng bo'ladi.

Kalitlarni boshqarishning yana bir asosiy jarayoni – *kalitlarni generatsiyalash* hisoblanadi. Masalan, shifrlash jarayoni uchun hujumchi noma'lum bo'lgan va uni bashorat qilish ehtimoli kam bo'lgan tasodifiy kalitlarni generatsiyalash talab etiladi. Tasodifiy kalitlarni generatsiyalash tasodifiy sonlarni yoki bitlar ketma-ketligini tanlashdan iborat bo'lib, amalga oshirishda yetarlicha murakkabliklarni taqdim etadi.

*Misol 1.6.1.* 0 va 1 lardan iborat bo'lgan tasodifiy ketma-ketlikni generatsiyalash uchun tangani to'g'ri tushgan holatini 1 deb, teskari holatini esa 0 deb olish mumkin. Agar tanga xolis deb hisoblanilsa, u holda tangani to'g'ri tushish ehtimoli ½ ga teng bo'ladi. Bu holat tangani qanday yasalganiga va tangani tashlash qanday amalga oshirilganiga bog'liq bo'ladi. Mazkur usul katta uzunlikdagi tasodifiy bitlar ketma-ketligini talab qiluvchi muhit uchun o'rinli hisoblanmaydi. Ushbu misol tasodifiylikka misol bo'la olsada, amaliy tomondan ahamiyatga ega hisoblanmaydi.

Tasodifiy ketma-ketliklarning haqiqiy manbasi fizik jihozlar bo'lgani bois, amalda ulardan foydalanish yuqori narx talab etishi yoki jarayon sekin amalga oshirilishi mumkin. Ushbu muammoni yechishda, amalda dastlabki kichik uzunlikdagi qiymatdan (*seed* deb nomlanadi) hisoblash asosida *psevdotasodifiy ketma-ketliklarni* generatsiyalash usulidan foydalaniladi. Agar psevdotasodifiy ketma-ketliklarni generatsiyalash usuli noma'lum bo'lganda, u to'liq tasodifiy ketma-ketliklarni generatsiyalashga imkon beradi. Biroq, kriptografik algoritmlarni yaratishda *Kerkgoff prinsiga* asoslanilgani bois, amalda bardoshli psevdotasodifiy ketma-ketliklarni generatsiyalash usullarini yaratish murakkab masalalardan hisoblanadi.

## 1.7. Kriptografik algoritmlarga qaratilgan hujumlar

Yuqorida simmetrik va ochiq kalitli kriptografik tizimlardan oydalanish sxemalarida hujumchi yoki passiv hujumchi atamalari eltirildi. Bundan tashqari, deshifrlash tushunchasi haqida ma'lumotlar eltirildi. Ushbu tushunchalar kriptotahlil deb nomlanuvchi fan hasiga tegishli bo'lib, ushbu bo'limda ularga qisqacha to'xtalib iladi.



*Ta'rif 1.7.1. Kriptoanaliz* – qanday ishlashini tushunish, ularni buzish yoki obro'sizlantirish usullarini topish hamda takomillashtirish maqsadida shifrmatn, shifrlash algoritmi yoki kriptotizimni o'rganish jarayoni.

Odatda kriptoanalizda asosiy maqsad sifatida shifrlash kalitini topish qaraladi. Hujumchilarning darajasiga ko'ra kriptografik hujumlar quyidagi turlarga ajratiladi:

1. *Passiv hujum*da hujumchiga faqat aloqa kanalini kuzatish imkoniyati beriladi va u asosan ma'lumotning konfidensialligini buzishga qaratiladi.

2. *Aktiv hujum*da hujumchi kanal orqali uzatilgan ma'lumotlarni o'chirishi, modifikatsiyalashi yoki almashtirishning boshqa usullaridan foydalanishi mumkin bo'ladi. Aktiv hujum ma'lumot yaxlitligi, konfidensiallini va autentifikatsiyasini buzishga qaratilgan bo'ladi.

Shifrlash sxemalari uchun shifrmatndan ochiq matnni olishni yoki shifrlash kalitini topishni maqsad qilgan quyidagi hujum usullari mavjud:

1. *Faqat shifrmatnga asoslangan hujum* faqat bir yoki bir nechta shifrmatnlar asosida ochiq matnni yoki shifrlash kalitini topishni maqsad qiladi. Ushbu hujumga bardoshsiz bo'lgan shifrlash algoritmi to'liq xavfsiz emas deb qaraladi.

2. *Ma'lum ochiq matnlarga asoslangan hujum* ma'lum sondagi ochiq matnlar va ularga mos bo'lgan shifrmatnlar asosida shifrlash kalitini topishni maqsad qiladi. Biroq, ko'p sonli ochiq matn va shifrmatn juftliklari kerak bo'lgani bois, ushbu hujumni amalga oshirish murakkab vazifa hisoblanadi.

3. *Tanlangan ochiq matnga asoslangan hujum* buzg'unchi tomonidan tanlangan ochiq matn va unga mos shifrmatn berilganda shifrlash kalitini topishni maqsad qiladi. Shundan so'ng, berilgan shifrmatnlar uchun ochiq matnni topish imkoniyati tug'iladi.

4. *Adaptiv tanlangan ochiq matnga asoslangan hujum* ham tanlangan ochiq matnga asoslangan hujum kabi bo'lib, ochiq matnni tanlanishi oldingi shifrmatnga bog'liq bo'lishi bilan farqlanadi.

5. *Tanlangan shifrmatnga asoslangan hujum* hujumchi tomonidan tanlangan shifrmatnga mos bo'lgan ochiq matn berilishi bilan xarakterlanadi.

*6. Adaptiv tanlangan shifrmatnga asoslangan hujum* ham tanlangan shifrmatnga asoslangan hujum kabi bo'lib, shifrmatnni tanlanishi oldingi ochiqmatnga bog'liq bo'lishi bilan farqlanadi.

Kriptografik algoritmlardan protokol ko'rinishida foydalanilgani bois, protokollarga qaratilgan hujumlarning ayrimlari quyida keltirilgan:

*1. Ma'lum kalit bo'yicha hujum.* Ushbu hujumda hujumchi oldin foydalanilgan kalitlar haqidagi ma'lumot asosida yangi kalitlarni hisoblaydi.

*2. Takrorlash hujumi.* Ushbu hujumda hujumchi o'rnatilgan aloqa seansini to'liq ko'chirib oladi va keyinchalik uni to'liqligicha yoki qisman takrorlaydi.

*3. Obro'sizlantirish hujumi.* Ushbu hujumda hujumchi tarmoqdagi qonuniy tomonlarning biri nomidan amallarni bajaradi.

*4. Lug'atga asoslangan hujum.* Ushbu hujum parolga qaratilgan bo'lib, bunda parollar faylida saqlangan parollarning xesh qiymatlariga mos haqiqiy parolni topishda keng tarqalgan parollar lug'atidan foydalanadi. Keng tarqalgan parollar lug'ati Internet tarmog'idagi ko'p sonli foydalanuvchilar tomonidan foydalanilgan eng ommabob parollardan tashkil topgan.

### Nazorat savollari

1. Axborot xavfsizligi va uning asosiy tushunchalari.
2. Kriptografik funksiyalar va ularning turlari.
3. Kriptografiyaning asosiy tushunchalari.
4. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalarga oid asosiy tushunchalar.
5. Ochiq kalitli kriptotizimlar va ularning vazifalari.
6. Zamonaviy kriptografiyaning bo'limlari.
7. Simmetrik kalitli shifrlarda foydalanilgan akslantirishlar.
8. Kriptografik protokol va uning vazifasi.
9. Kriptografik kalitlarni boshqarish bo'limi va unga oid asosiy muolajalar.
10. Kriptografik algoritmlarga qaratilgan hujum turlari.
11. Kriptotahlil fan sohasi va uning maqsadi.
12. Axborotni himoyalashda kriptografiyaning o'rnini asoslang.
13. Bir tomonlama funksiya va uning xususiyatlari.



## 2 BOB.
## KRIPTOGRAFIYANING MATEMATIK ASOSI

Ushbu bo'lim kriptografiyaning matematik asosiga bag'ishlanadi. Shu sababli ularni boshlashdan oldin umumiy standart ko'rinishdagi belgilanishlarni keltirish maqsadga muvofiq:

- $\mathbb{Z}$ – *butun sonlar to'plamini* ifodalaydi: $\{\dots,-2,-1,0,1,2,\dots\}$.
- $\mathbb{Q}$ – *ratsional sonlar to'plamini* ifodalaydi: $\left(\frac{a}{b}\middle| a,b\in\mathbb{Z},b\neq 0\right)$.
- $\mathbb{R}$ – *real sonlar to'plamini* ifodalaydi.
- $\pi$ – matematik o'zgarmas, $\pi\approx 3.14159$.
- $e$ – natural logarifm asosi, $e\approx 2.71828$.
- $[a,b]$ – belgilanish $a\le x\le b$ shartni qanoatlantiruvchi $x$ butun sonni ifodalaydi;
- $\lfloor x\rfloor$ – belgilanish $x$ ga teng yoki undan kichik eng katta butun sonni ko'rsatadi. Masalan, $\lfloor 5.2\rfloor = 5$ va $\lfloor -5.2\rfloor = -6$.
- $\lceil x\rceil$ – belgilanish $x$ ga teng yoki undan katta eng kichik butun sonni ko'rsatadi. Masalan, $\lceil 5.2\rceil = 6$ va $\lceil -5.2\rceil = -5$.
- $[x]$ – belgilanish $x$ ning butun qismini ko'rsatadi. Masalan, $[5.2] = 5$, va $[5.8] = 5$.
- Agar $A$ chekli to'plam bo'lsa, $A$ dagi elementlar soni $|A|$ bilan belgilanadi.
- $a\in A$ – element $a$ ning to'plam $A$ ga tegishligini anglatadi.
- $A\subseteq B$ – to'plam $A$ to'plam $B$ ning qism to'plami ekanligini anglatadi.
- $A\subset B$ – to'plam $A$ to'plam $B$ ning mos qismto'plami, ya'ni: $A\subseteq B$ va $A\neq B$.
- $A$ va $B$ to'plamlarning *kesishmasi* bo'lgan to'plam $A\cap B = \{x\mid x\in A\ va\ x\in B\}$ bilan belgilanadi.
- $A$ va $B$ to'plamlarning *birlashmasi* bo'lgan to'plam $A\cup B = \{x\mid x\in A\ yoki\ x\in B\}$ bilan belgilanadi.
- $A$ va $B$ to'plamlarning *farqi* bo'lgan to'plam $A-B=\{x\mid x\in A\ va\ x\notin B\}$ bilan belgilanadi.
- $A$ va $B$ to'plamlarning Dekart ko'paytmasi $A\times B = \{(a,b)|a\in A\ va\ b\in B\}$ bilan belgilanadi. Masalan, $\{a_1,a_2\}\times\{b_1,b_2,b_3\} = \{(a_1,b_1),(a_1,b_2),(a_1,b_3),(a_2,b_1),(a_2,b_2),(a_2,b_3)\}$.

- *Funksiya* yoki *akslantirish* $f: A \to B$ – $A$ to'plamning har bir $a$ elementini $B$ to'plamning aniq bir $b$ elementiga o'zlashtiruvchi qoida. Agar $a \in A$ element $b \in B$ elementga akslantirilsa, $b$ element $a$ elementning *aksi*, $a$ element esa $b$ elementning *asli* deb ataladi va $f(a) = b$ shaklida ifodalanadi. $A$ to'plam $f$ funksiyaning *aniqlanish sohasi*, $B$ to'plam esa $f$ funksiyaning *qiymatlar sohasi* deb ataladi.

- Agar $B$ to'plamdagi har bir element $A$ to'plamda ko'pi bilan bir elementning aksi bo'lsa, $f: A \to B$ funksiya *birga-bir (1-1* yoki *injektiv)* funksiya deb aytiladi. Shuning uchun $f(a_1) = f(a_2)$ deyilganda $a_1 = a_2$ nazarda tutiladi.

- Agar har bir $b \in B$ kamida bitta $a \in A$ ning aksi bo'lsa, u holda $f: A \to B$ - *ustiga (*yoki *surjektiv)* funksiya deyiladi.

- Agar $f: A \to B$ funksiya ham birga-bir ham ustiga funksiya bo'lsa, u holda *bijektiv* funksiya funksiya deb ataladi. Agar $f$ funksiya $A$ va $B$ to'plamlar orasida bijektiv bo'lsa, u holda $|A| = |B|$ tenglik o'rinli. Agar $f$ funksiya $A$ va o'zining o'rtasida bijektiv bo'lsa, $f$ funksiya $A$ to'plamda *o'rin almashtirish funksiyasi* deb aytiladi.

- $\ln x - x$ ning natural logarifmi, ya'ni, $e$ asosga ko'ra $x$ ning logarifmi.

- $\lg x - 2$ asosga ko'ra $x$ ning logarifmi.

- $\exp(x) - e^x$ eksponent funksiya.

- $\sum_{i=1}^{n} a_i$ ifoda $a_1 + a_2 + \cdots + a_n$ yig'indini ifodalaydi.

- $\prod_{i=1}^{n} a_i$ ifoda $a_1 \cdot a_2 \cdots a_n$ ko'paytmani ifodalaydi.

- Musbat $n$ soni uchun $n! = n(n-1)(n-2)\cdots 1$ – faktorial funksiyasini ifodalaydi. Shartli holatda, $0! = 1$ ga teng.

## 2.1. Ehtimollar nazariyasi asoslari

*Ta'rif 2.1.1. Tajriba* – bu ma'lum natijalar to'plamidan birini beruvchi protsedura bo'lib, mumkin bo'lgan individual natijalar *oddiy hodisalar* deb ataladi. Barcha mumkin bo'lgan natijalar to'plami esa *na'munalar maydoni* deb ataladi.

Mazkur bo'limda faqat chekli sondagi natijalarga ega bo'lgan – *diskret* na'munalar maydoni ko'rib chiqiladi. Faraz qilaylik, $S$ na'munalar maydonidagi oddiy hodisalar $s_1, s_2, \ldots, s_n$ kabi belgilansin.

*Ta'rif 2.1.2.* $S$ maydonda $P$ *ehtimollik taqsimoti* – manfiy bo'lmagan va yig'indisi 1 ga teng bo'lgan $p_1, p_2, \ldots, p_n$ sonlar ketma –



ketligi bo'lib, $p_i$ kattalik tajriba natijasini $s_i$ hodisa bo'lish ehtimolini ko'rsatadi.

*Ta'rif 2.1.3. Hodisa* $E$ na'munalar maydoni $S$ ning qism to'plami bo'lsin. $E$ hodisaning paydo bo'lish *ehtimoli* – $P(E)$ kabi belgilanib, $E$ hodisaga tegishli bo'lgan barcha $s_i$ sodda hodisalarning $p_i$ ehtimolliklarining yig'indisi hisoblanadi. Agar $s_i \in S$ bo'lsa, $P(\{s_i\})$ ehtimollikni $P(s_i)$ kabi belgilash mumkin.

*Ta'rif 2.1.4.* Agar $E$ hodisa bo'lsa, unga *teskari hodisa* $\bar{E}$ kabi belgilanadi va $E$ ga tegishli bo'lmagan sodda hodisalar to'plamini ifodalaydi.

Faraz qilaylik, $E \subseteq S$ hodisa bo'lsin.

I. $0 \le P(E) \le 1$. Bundan tashqari, $P(S) = 1$ va $P(\emptyset) = 0$ (bu yerda, $\emptyset$ - bo'sh to'plam).

II. $P(\bar{E}) = 1 - P(E)$.

III. Agar $S$ maydondagi natijalar teng darajada bo'lsa, u holda $P(E) = \frac{|E|}{|S|}$ o'rinli.

*Ta'rif 2.1.5.* Agar $P(E_1 \cap E_2) = 0$ o'rinli bo'lsa, u holda ikki $E_1$ va $E_2$ hodisalar bir-birini inkor etuvchi deb ataladi. Ya'ni, ikkita hodisadan birining sodir bo'lishi, boshqasining sodir bo'lish ehtimolini inkor qiladi.

Faraz qilaylik, $E_1$ va $E_2$ ikki turli hodisa bo'lsin. U holda quyidagilar o'rinli:

I. Agar $E_1 \subseteq E_2$ bo'lsa, u holda $P(E_1) \le P(E_2)$ o'rinli bo'ladi.

II. $P(E_1 \cup E_2) + P(E_1 \cap E_2) = P(E_1) + P(E_2)$. Shu sababli, agar $E_1$ va $E_2$ lar bir-birini inkor etuvchi bo'lsa, u holda $P(E_1 \cup E_2) = P(E_1) + P(E_2)$ o'rinli bo'ladi.

*Shartli ehtimollik*

*Ta'rif 2.1.6.* Faraz qilaylik, $E_1$ va $E_2$ lar $P(E_2) > 0$ ehtimolikka ega bo'lgan ikki turli hodisa bo'lsin. Berilgan $E_2$ hodisa paydo bo'lganda $E_1$ hodisaning paydo bo'lishining *shartli ehtimoli* $P(E_1|E_2)$ kabi belgilanadi va u quyidagiga teng:

$$P(E_1|E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)}$$

*Ta'rif 2.1.7.* Agar $P(E_1 \cap E_2) = P(E_1)P(E_2)$ bo'lsa, $E_1$ va $E_2$ hodisalar *mustaqil* deb aytiladi.

Yuqoridagi ta'rifdan kelib chiqib, agar $E_1$ va $E_2$ hodisalar mustaqil bo'lsa, u holda $P(E_1|E_2) = P(E_1)$ va $P(E_2|E_1) = P(E_2)$ o'rinli bo'ladi.

*Bayes teoremasi.* Agar $E_1$ va $E_2$ lar $P(E_2) > 0$ ehtimolikka ega ikki turli hodisa bo'lsa, u holda quyidagi tenglik o'rinli:

$$P(E_1|E_2) = \frac{P(E_1)P(E_2|E_1)}{P(E_2)}$$

*Binomial taqsimot*

*Binomial koeffitsient xususiyatlari.* Faraz qilaylik, $n$ va $k$ manfiy bo'lmagan butun sonlar bo'lsin. U holda quyidagilar o'rinli bo'ladi:

I. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

II. $\binom{n}{k} = \binom{n}{n-k}$.

III. $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

*Tug'ilgan kun muammosi*

Musbat $m$, $n$ $(m \geq n)$ butun sonlar uchun, $m^{(n)}$ butun son quyidagicha hisoblanadi:

$$m^{(n)} = m(m-1)(m-2)\cdots(m-n+1).$$

$m$, $n$ $(m \geq n)$ manfiy bo'lmagan butun sonlar bo'lsin. *Ikkinchi turdagi Stirling raqami* - $\left\{ {m \atop n} \right\}$ kabi belgilanib, quyidagiga teng:

$$\left\{ {m \atop n} \right\} = \frac{1}{n!}\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^m,$$

Bu yerda, $\left\{ {0 \atop 0} \right\} = 1$ holat bundan mustasno.



$\left\{ {m \atop n} \right\}$ belgilanish $m$ obyektlar to'plamini $n$ bo'sh bo'lmagan qismto'plamlarga bo'lish yo'llari sonini ifodalaydi.

*Klassik bandlik muammosi.* Ko'zada 1 dan $m$ gacha raqamlangan $m$ ta sharcha mavjud. Faraz qilaylik, ko'zadan aralashtirish yo'li bilan birin-ketin $n$ ta sharcha tortib olindi va ularning raqamlari qayd etildi. Bu holda, turli $t$ sharning tanlanish ehtimoli quyidagiga teng:

$$P_1(m,n,t) = \left\{ {n \atop t} \right\}\frac{m^{(t)}}{m^n}, \qquad 1 \leq t \leq n.$$

Tug'ilgan kun muammosi ham klassik muammoning bir xususiy holati hisoblanadi.

*Tug'ilgan kun muammosi.* Ko'zada 1 dan $m$ gacha raqamlangan $m$ ta sharcha mavjud. Faraz qilaylik, ko'zadan birin-ketin aralashtirish yo'li bilan $n$ ta sharcha tortib olindi va ularning raqamlari qayd etildi.

I. Tanlashdagi kamida bir marta takrorlanish ehtimoli (ya'ni, kamida ikkita sharcha tanlanganda) quyidagiga teng:

$$P_2(m,n) = 1 - P_1(m,n,n) = 1 - \frac{m^{(n)}}{m^n}, \qquad 1 \leq n \leq m. \tag{2.1}$$

Agar $n = O(\sqrt{m})$ (2.3-bo'limga qarang) va $m \to \infty$, u holda:

$$P_2(m,n) \to 1 - \exp\left(-\frac{n(n-1)}{2m} + O\left(\frac{1}{\sqrt{m}}\right)\right) \approx 1 - \exp\left(-\frac{n^2}{2m}\right)$$

II. $m \to \infty$ ni inobatga olib, bir xil sharcha takrorlanishidan oldingi kutiladigan tanlashlar soni $\sqrt{\frac{\pi m}{2}}$ ga teng bo'ladi.

Yuqoridagi holatni nima uchun *tug'ilgan kun muammosi* deb atalishiga qisqacha izoh bersak. 23 kishilik xonada kamida 2 kishining tug'ilgan kuni bir xil bo'lish ehtimoli $P_2(365,23) \approx 0.507$ ga teng bo'lib, u yetarlicha katta hisoblanadi. Bundan tashqari, $P_2(365,n)$ miqdor $n$ ning ortishi bilan tez ko'payadi; masalan, $P_2(365,30) \approx 0.706$.

Faraz qilaylik, $X$ tasodifiy o'zgaruvchi bo'lib, $P(X = x_i) = p_i$ ehtimollikga ega $x_1, x_2, \dots, x_n$ chekli sondagi qiymatlar to'plamidan iborat bo'lsin. Bu yerda, har bir $i$ $(1 \le i \le n)$ uchun $0 \le p_i \le 1$ o'rinli va $\sum_{i=1}^{n} p_i = 1$ ga teng. Shuningdek, $Y$ va $Z$ lar ham tasodifiy o'zgaruvchi bo'lib, chekli sondagi qiymatlar to'plamidan iborat.

Informatsiyaning statistik nazariyasi K.Shennon tomonidan batafsil o'rganilgan.

Yuz berish ehtimolligi birga yaqin bo'lgan tez-tez uchraydigan hodisa xususida xabar paydo bo'lsa, bunday xabarning qabul qiluvchi uchun informativligi kam bo'ladi. Xuddi shunday yuz berish ehtimolligi nolga yaqin bo'lgan xabarning ham informativligi kam bo'ladi.

Hodisalarga qandaydir tajribaning natijasi sifatida qarash mumkinki, bunday tajribaning barcha natijalari ansamblni, ya'ni hodisalarning to'liq guruhini tashkil etadi. K.Shennon tajriba jarayonida paydo bo'luvchi hodisaning *noaniqligi* tushunchasini kiritdi va uni *entropiya* deb atadi.

Ansambl entropiyasi uning noaniqligining va demak informativligining miqdoriy o'lchovi bo'lib, tajribaning har bir mumkin bo'lgan natijalari ehtimolligi to'plamining o'rtacha funksiyasi sifatida ifodalanadi.

*Ta'rif 2.2.1.* $X$ o'zgaruvchining *noaniqligi* yoki *entropiyasi* $H(X) = -\sum_{i=1}^{n} p_i \lg p_i = \sum_{i=1}^{n} p_i \lg\left(\frac{1}{p_i}\right)$ kabi belgilanib, shartli ravishda, agar $p_i = 0$ bo'lsa, $p_i \lg p_i = p_i \lg\left(\frac{1}{p_i}\right) = 0$ tenglik o'rinli.

*Entropiyaning xususiyatlari.* Faraz qilaylik, $X$ kattalik $n$ ta qiymatdan iborat o'zgaruvchi bo'lsin. U holda quyidagilar o'rinli:

I. $0 \le H(X) \le \lg n$;

II. Faqat $i$ ning biror qiymati uchun $p_i = 1$ va qolgan barcha $i \ne j$ uchun $p_j = 0$ bo'lsa, $H(X) = 0$ ga teng bo'ladi (ya'ni, natijaning noaniqligi yo'q).

III. Faqat $i$ ning $(1 \le i \le n)$ har bir qiymati uchun $p_i = 1/n$ o'rinli bo'lsa, $H(X) = \lg n$ ga teng bo'ladi.

Birlashma entropiya statistik bog'langan xabarlarning birgalikda paydo bo'lish entropiyasini hisoblashda ishlatiladi.



*Ta'rif 2.2.2.* $X$ va $Y$ larning *birlashma entropiyasi* quyidagiga teng:

$$H(X,Y) = -\sum_{x,y} P(X = x, Y = y) \lg\big(P(X = x, Y = y)\big),$$

bu yerda, yig'indi $x$ va $y$ larni mos holda $X$ va $Y$ larning qiymatlari sohasida tegishligini bildiradi. Ifodani ixtiyoriy sondagi tasodifiy o'zgaruvchilar uchun ham ifodalash mumkin.

Agar $X$ va $Y$ lar tasodifiy o'zgaruvchilar bo'lsa, u holda $H(X,Y) \le H(X) + H(Y)$ shart faqat va faqat $X$ va $Y$ lar mustaqil bo'lganda o'rinli bo'ladi.

Entropiyalarni jamlash qoidasiga muvofiq ikkita mazmun jihatidan turli (mustaqil) kitoblardagi informatsiya miqdori – alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng. Agar bir kitob ikkinchi kitobning qismini o'z ichiga olsa, ushbu ikki kitobdagi informatsiya miqdori alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng bo'lmaydi, balki undan kam bo'ladi. Bu holda informatsiya miqdorini o'lchashda *shartli entropiya* tushunchasidan foydalaniladi. Shartli entropiyani hisoblashda shartli ehtimolliklar u yoki bu ko'rinishda ishlatiladi.

*Ta'rif 2.2.3.* Agar $X$ va $Y$ lar tasodifiy o'zgaruvchilar bo'lsa, *berilgan* $Y = y$ *uchun* $X$ *ning shartli entropiyasi* quyidagicha ifodalanadi:

$$H(X|Y = y) = -\sum_x P(X = x|Y = y) \lg(P(X = x|Y = y)),$$

bu yerda, yig'indi $x$ qiymat $X$ ning qiymatlari sohasida tegishligini bildiradi.

Shartli entropiya quyidagi xususiyatlarga ega:

I. $H(X|Y)$ miqdor $Y$ hodisa kuzatilganidan so'ng $X$ ning noma'lumlik darajasi miqdorini o'lchaydi.

II. $H(X|Y) \ge 0$ va $H(X|X) = 0$.

III. $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$.

$H(X|Y) \le H(X)$ shart faqat va faqat $X$ va $Y$ lar mustaqil bo'lganda o'rinli bo'ladi.

dastur yordamida elektron darsliklar, CD/DVD tashrifnomalar, taqdimot va soddda o'yinlar yaratish mumkin.

Dasturning eng qulay tomoni dasturlash tillari bilan notanish foydalanuvchilar ham undan muvofaqqiyatli foydalanishlari mumkin. C++, Java, Visual Basic dasturlash texnologiyalaridan xabardor shaxslar uchun bu dasturning imkoniyatlari yanada kengroqdir.

AutoPlay Media Studio 8.0.6.0. dasturi bilan ishlash uchun minimal talablar:

- Operatsion tizim: Windows 2000, Windows XP, Windows Vista,
- Windows 7 va undan yangilari.
- Prosessor Pentium 4 va undan yangilari.
- OXS 256 MB yoki undan yuqori.
- Ekran sig'imi 1024x768 piksel va undan yuqori.
- Ranglar sifati 16 bit yoki undan yuqori.
- Xotirada o'rnatish uchun bo'sh joy sig'imi 100 MB.
- DirectX 7 va undan yangilari.
- Internet Explorer 4.0 va undan yangilari.
- Adobe Flash Player 8 va undan yangilari.
- Adobe Reader 8 va undan yangilari.

### *O'quv dasturlarini yaratish texnologiyasiga qo'yilgan talablar*

Elektron o'quv qo'llanma tizimidan foydalanuvchi samarali foydalanishi uchun tizim interfeysi sodda va tushunarli bo'lishi kerak.

Ekranda axborotlarni aks ettirishda quyidagi talablar qo'yiladi:

– ekranda aks ettiriladigan axborot tushunarli, mantiqan bog'langan, mazmuni va maqsadiga ko'ra guruhlarga ajratilgan bo'lishi kerak;

– axborotlarni tashkil etishda ortiqcha kodlashtirish va noto'g'ri, tushunarsiz qisqartmalardan foydalanmaslik kerak;

–foydalanuvchi uchun odatiy bo'lgan atamalar o'rniga axborot texnologiyalariga oid atamalardan foydalnishni minimallashtirish;



– axborotlarni aks ettirishda ekranning chetki qismlaridan foydalanmaslik;

– ekranda faqat foydalanuvchi ayni paytda qayta ishlayotgan axborot bo'lishi kerak;

Hozirgi paytda elektron o'quv qo'llanmalarga quyidagi talablar qo'yilmoqda:

1. Tanlangan kurs bo'yicha axborotlar yaxshi strukturalashtirilgan va tugallangan bo'lishi kerak;

2. Har bir qism axborotni matn bilan birga audio va video ko'rinishda taqdim etishi kerak.

3. Murakkab model yoki qurilmalarni tasvirlab beradigan rasmlarda kursor rasmning elementlari boylab harakatlanganda unga sinxron ravishda paydo bo'ladigan va yo'qoladigan shu element haqida ma'lumot beradigan tushuntirishlar bo'lishi kerak;

4. Matnli qism kerakli axborotni izlash vaqtini qisqartirish uchun ko'plab gipermatnlarga, shuningdek qidiruv tizimiga ega bo'lishi kerak.

5. Oddiy holatda tushunish qiyin bo'lgan bo'limlar videoma'lumotlar va animatsiyalar bilan boyitilishi kerak. Bu holda axborotni qabul qilish uchun ketadigan vaqt an'anaviy o'quv qo'llanmalarga qaraganda 5-10 marotabagacha qisqarishi mumkin;

6. Audioma'lumotlarning bo'lishi muayan mavzularni o'zlashtirishda juda samarali hisoblanadi.

Elektron o'quv qo'llanmalar 3 ta asosiy rejimda ishlashi mumkin:

✓ Sinovsiz o'rgatish

✓ Sinovli o'rgatish. Bu holda har bir bob (mavzu) oxirida foydalanuvchi shu bob (mavzu)ni qanchalik darajada o'zlashtirganligini aniqlash ushun bir qancha savollarga javob berish taklif etiladi

✓ Test nazorati o'rganilgan kurs bo'yicha o'zlashtirish darajasini aniqlash uchun mo'ljallangan

Elektron o'quv qo'llanma tarkibiga nazorat vositalari ham bo'lishi kerak, chunki bilimlarni nazorat qilish ta'lim jarayonidagi asosiy muammolardan biri

hisoblanadi. Hozirga qadar ta'lim tizimida bilimlarni nazorat qilishning og'zaki va yozma shakllaridan foydalanilgan. Hozirgi paytda esa turli xil test o'tkazish usullaridan foydalanilmoqda. Ma'lumki biror bir predmet sohani samarali egallash uchun nazariy qismini o'rganish bilan birga masalalarni yechish uchun amaliy ko'nikmalarga ham ega bo'lish kerak. Buning uchun o'rganilayotgan jarayon va hodisalarning fizik modellarini qurish, masalani yechish algoritmlari va dasturlarini loyihalashni o'rganish kerak. Bularni amalga oshirish uchun elektron o'quv qo'llanma tarkibiga turli xil grafik va dasturiy vositalar kiritilishi mumkin.

**Nazorat savollari**

1. Elektron ta'lim nima?
2. Elektron o'quv kursi haqida izohlang.
3. Elektron o'quv dasturlarini yaratish texnologiyasi va dasturiy ta'minoti haqida izohlang.
4. O'quv dasturlarini yaratish texnologiyasiga qo'yilgan talablar nimalardan iborat?



# II BOB. PROFESSIONAL VA DUAL TA'LIM TIZIMINI TASHKIL ETISH. ELEKTRON TA'LIMNI TASHKIL QILISH SHAKLLARI VA USULLARI

## 2.1. Professional va Dual ta'lim tizimi

### *Professional ta'lim tizimi mazmuni*

Kasb-hunar maktablari, kollejlar va texnikumlarga idoraviy bo'ysunuvidan qat'i nazar o'quv-metodik rahbarlik qilish hamda bu sohada davlat siyosatini yuritish Oliy va o'rta maxsus ta'lim vazirligi tomonidan amalga oshiriladi.

Boshlang'ich, o'rta va o'rta maxsus professional ta'lim tizimida tegishli ta'lim dasturlari joriy etilgan kasb-hunar maktablari, kollejlar va texnikumlardan iborat professional ta'lim muassasalari tarmog'i tashkil etiladi.

Jumladan,

– ***kasb-hunar maktablarida***: maktablarning 9-sinf bitiruvchilariga 2 yillik umumta'lim va mutaxassislik fanlarining integratsiyalashgan dasturlari asosida kunduzgi ta'lim beriladi;ta'lim olayotgan o'quvchilar Davlat byudjeti hisobidan bazaviy hisoblash miqdorining bir baravari miqdorida oylik stipendiya hamda uch mahal ovqat bilan ta'minlanadi.

– ***kollejlarda***:

kamida umumiy o'rta ma'lumotga ega bo'lgan shaxslarga kasblar va mutaxassisliklarning murakkabligidan kelib chiqqan holda 2 yilgacha muddatda kunduzgi, kechki va sirtqi ta'lim shakllarida davlat buyurtmasi hamda to'lov-kontrakt asosida ta'lim beriladi.

– ***texnikumlarda***:

umumiy o'rta ma'lumotga ega bo'lgan shaxslarga kasblar va mutaxassisliklarning murakkabligidan kelib chiqqan holda 2 yildan kam bo'lmagan muddatda kunduzgi, kechki va sirtqi ta'lim shakllarida davlat buyurtmasi hamda to'lov-kontrakt asosida ta'lim beriladi;

texnikumlarni tamomlagan bitiruvchilar o'z sohasiga mos bakalavriat ta'lim yo'nalishlari bo'yicha kirish imtihonlarisiz yakka tartibdagi suhbat orqali oliy ta'lim muassasalarida 2-kursdan o'qishini davom ettirish huquqiga ega bo'ladi.

1. Boshlang'ich professional ta'lim bosqichida kadrlar tayyorlaydigan ta'lim muassasalari (Kasb-hunar maktablari) ro'yxati

2. O'rta professional ta'lim bosqichida kadrlar tayyorlaydigan ta'lim muassasalari (kollejlar) ro'yxati

3. Oliy ta'lim muassasalari huzurida tashkil etiladigan texnikumlar ro'yxati

**Professional ta'lim muassasasining vazifalari, huquqlari hamda majburiyatlari**

**Professional ta'lim muassasasi vazifalari:**

- tashkilot bilan birgalikda o'quvchilarni o'qishga qabul qilish boshlanishidan kamida bir oy oldin dual ta'lim bo'yicha tegishli shartnomalarni rasmiylashtiradi;

- tashkilot bilan birgalikda kasb va mutaxassisliklar bo'yicha tegishli vazirliklar va idoralar bilan kelishgan holda tasdiqlangan ta'lim dasturlari asosida dual ta'lim bo'yicha o'quv-metodik hujjatlarni ishlab chiqadi va tasdiqlaydi;

- tashkilot bilan dual ta'lim muddati hamda o'quvchilarning ro'yxatini tasdiqlaydi;

- o'quvchi va tashkilot o'rtasida dual ta'lim bo'yicha tuzilgan shartnomalarni ro'yxatga oladi;

- qonun hujjatlariga muvofiq shartnomasi mavjud o'quvchilarni dual ta'lim bo'yicha guruhlarga qabul qilishni tashkil etadi;

- dual ta'limni tashkil etish, o'quvchilarni tashkilotga yuborish, o'quvchilarning har bir guruhiga ishlab chiqarish ta'limi ustasi yoki o'qituvchini buyruq asosida biriktiradi;

- dual ta'lim dasturini amalga oshirishni ta'minlaydi;

- tashkilot bilan o'quvchilarni baholashni va yakuniy davlat attestatsiyasini belgilangan tartibda tashkil etadi;

- tashkilot bilan kelishgan holda dual ta'lim yuzasidan hisobotlarni tayyorlaydi va tegishli vazirliklar va idoralar hamda Kasbiy ta'limini rivojlantirish va muvofiqlashtirish hududiy boshqarmalariga taqdim etadi;



- dual ta'lim bo'yicha tegishli vazirliklar va idoralarning buyruqlari va ko'rsatmalarini o'z vaqtida bajaradi.

Professional ta'lim muassasasi qonun hujjatlariga muvofiq boshqa vazifalarni ham bajarishi mumkin.

**Professional ta'lim muassasasi quyidagi huquqlarga ega:**

- dual ta'limning amaliy qismi o'tilishi bo'yicha tashkilotga murojaat qilish;

- dual ta'lim sifatini oshirish yuzasidan tashkilotga takliflar berish;

- dual ta'lim jarayonini tashkil etish uchun tuzilgan shartnomalarga tomonlar bilan kelishgan holda o'zgartirishlar kiritish;

- O'zbekiston Respublikasi hududida o'z nomidan yuridik shaxslar bilan vakolati doirasida dual ta'limni tashkil etish bo'yicha shartnomalar va boshqa hujjatlar tuzish;

- dual ta'lim bo'yicha to'lov-kontrakt asosida o'qitishdan tushadigan hamda qonun hujjatlarida taqiqlanmagan boshqa manbalardan tushgan mablag'larni professional ta'lim muassasasining moddiy-texnik bazasini mustahkamlashga va ta'lim-tarbiya jarayonini zamonaviy o'quv-texnik vositalar, mebellar bilan ta'minlashga, o'qituvchilar va ishlab chiqarish ta'limi ustalari, xodimlarni ijtimoiy himoyalashga va ularning faoliyati samaradorligini oshirishni rag'batlantirishga sarflash huquqiga ega.

Professional ta'lim muassasasi qonun hujjatlariga muvofiq boshqa huquqlarga ham ega bo'lishi mumkin.

**Professional ta'lim muassasasi o'ziga quyidagi majburiyatlarni oladi:**

o'qituvchilar va ishlab chiqarish ta'limi ustalari faoliyatini nazorat qilish;

iqtisodiyot tarmoqlari va xizmat ko'rsatish sohasida kadrlarga bo'lgan real ehtiyoj asosida dual ta'limni tashkil etish bo'yicha tashviqot va targ'ibot ishlarini olib borish;

o'quvchi kundaligini nazorat qilish.

Professional ta'lim muassasasi qonun hujjatlariga muvofiq boshqa majburiyatlarni ham bajarishi mumkin.

**O‘quvchilarning vazifalari:**

tashkilotning ustaviga muvofiq ish jarayonlarida belgilangan tartibda qatnashadi;

o‘quv mashg‘ulotlariga nazariy, o‘quv va amaliy qismi bo‘yicha qatnashadi;

dual ta’lim jarayoni so‘ngida yakuniy davlat attestatsiyasini topshiradi.

O‘quvchilar qonun hujjatlariga muvofiq boshqa vazifalarni ham bajarishi mumkin.

**O‘quvchilar quyidagi huquqlarga ega:**

tegishli kasb yoki mutaxassislik bo‘yicha bilim olish;

o‘quv, texnika jihozlari va vositalaridan, fan kabinetlari axborot-kutubxonasi fondidan, axborot-kutubxona o‘quv zali va boshqa o‘quv, yordamchi xonalardan, sport majmualari, professional ta’lim muassasasiga qarashli tibbiy va texnik jihozlardan bepul foydalanish;

tashkilotda amaliyot bazalaridan, tashkilotning moddiy-texnik bazasidan foydalanish;

tashkilotdagi mehnat va jamoat ishlarida qatnashish;

dual ta’lim vaqtida tashkilotdan shartnomaga muvofiq ish haqi olish.

O‘quvchilar qonun hujjatlariga muvofiq boshqa huquqlarga ham ega bo‘lishi mumkin.

**O‘quvchilar o‘z zimmasiga quyidagi majburiyatlarni oladi:**

tashkilot va professional ta’lim muassasasida belgilangan tartib va qoidalarga rioya qilish;

dual ta’lim jarayonida professional ta’lim muassasasi va tashkilot tomonidan berilgan vazifalarni o‘z vaqtida bajarish;

o‘quvchi kundaligini o‘z vaqtida yuritib borish va hisobotlarni topshirish.

O‘quvchilar qonun hujjatlariga muvofiq boshqa majburiyatlarni ham bajarishi mumkin.



**Professional ta’lim tizimida dual ta’limni tashkil etish**

**SXEMASI**

| Bosqichlar | Subyektlar | Tadbirlar | Muddatlar |
|---|---|---|---|
| 1-bosqich | Qoraqalpog‘iston Respublikasi Vazirlar Kengashi, viloyatlar va Toshkent shahar hokimliklari, manfaatdor vazirliklar va idoralar | 1. O‘rta bo‘g‘in kadrlariga bo‘lgan ehtiyojni aniqlash va ularga qo‘yiladigan talablarni belgilash.<br>2. Dual ta’lim bo‘yicha kadrlar tayyorlashda ishtirok etadigan tashkilotlar bo‘yicha taklif tayyorlash. | Har yili 1-martga qadar |
| 2-bosqich | Oliy va o‘rta maxsus ta’lim vazirligi, manfaatdor vazirliklar va idoralar | Dual ta’lim bo‘yicha kadrlar tayyorlaydigan professional ta’lim muassasalarini belgilash. | Har yili 1-iyulga qadar |
| | | 1. Dual ta’limni tashkil etish va muvofiqlashtirish bilan bog‘liq choralar ko‘rish.<br>2. Professional ta’lim muassasalarida dual ta’limni tashkil etish yuzasidan monitoring olib borish. | O‘quv yili mobaynida |
| 3-bosqich | Professional ta’lim muassasalari, tashkilotlar | 1. Dual ta’limni amalga oshirish bo‘yicha shartnoma tuzish.<br>2. Kasbga yo‘naltirish ishlarini amalga oshirish hamda dual ta’lim bo‘yicha o‘quvchilar qabulini tashkil etish.<br>3. Dual ta’limni tashkil etish bo‘yicha o‘quv jarayoni grafigini ishlab chiqish. | O‘quv jarayoni boshlanishidan kamida bir oy oldin |
| 4-bosqich | Tashkilotlar | 1. O‘qitishning amaliy qismini tashkilotda tashkil etish. | O‘quv yili mobaynida |

| | | | |
|---|---|---|---|
| | | 2. O‘quvchiga belgilangan tartibda ish haqi to‘lash. | |
| 5-bosqich | Professional ta’lim muassasalari, tashkilotlar | 1. Tashkilotlar bilan shartnoma imzolagan o‘quvchilarni o‘qishga qabul qilish.<br>2. Dual ta’limning nazariy qismini tashkil etish. | O‘quv yili mobaynida |

***Dual ta’limni tashkil etish***

Dual tizim - talaba nazariy bilimlarni ta'lim muassasasida, amaliy ko‘nikmalarni esa ish joyida oladigan o‘qitish turidir.

"Dual ta'lim" o‘rta kasb-hunar ta'limi sohasidagi eng mashhur jahon brendidir. Tarixan Germaniya, Avstriya va Shveytsariyada paydo bo‘lgan dual ta'lim kasbiy ta'lim dasturlarini ikki tomonlama institutsional birlashtirishni o‘z ichiga oladi: talabalar odatda dasturning nazariy qismini ta'lim tashkilotida, amaliy qismini esa - ish joyida, haqiqiy ishlab chiqarish jarayonida oladilar.

Dual ta'lim korxonada (tashkilotda) o‘qitishning o‘quv va amaliy qismini ishlab chiqishni o‘z ichiga oladi.

Kasb-hunar ta'limining dual tizimi konsepsiyasi ta'lim va ishlab chiqarish jarayonlarini sintez qilish orqali mutaxassislar tayyorlashda amaliy yo‘nalishni kuchaytirishga asoslangan bo‘lib, bu ta'lim muassasalari bitiruvchilarining kasbiy harakatchanligi imkoniyatlarini sezilarli darajada oshiradi. Dual tizim – turli faoliyat sohalaridagi korxonalar tomonidan bozor iqtisodiyotining zamonaviy sharoitida talabga ega bo‘lgan yuqori malakali mutaxassislarni tayyorlash imkonini beruvchi samarali va moslashuvchan mexanizm. Hech bir ta'lim dual ta'lim kabi ishlab chiqarishga oid bilimlarni ichkaridan bera olmaydi, bu uni muvaffaqiyatli martaba yo‘lida muhim qadam qiladi.

U tadbirkorlik sohasida yoshlar, ayniqsa, ayollar bandligini ta’minlash, malakali kadrlar tayyorlash va qashshoqlikni kamaytirish maqsadida tashkil etiladi.



Dastur tufayli ishlab chiqarish jarayonini bevosita korxonada (tashkilotda) o‘rganishni tashkil etish rejalashtirilgan.

Dual ta’lim bir necha bosqichda joriy etilishi rejalashtirilgan:

- Qoraqalpog‘iston, Toshkent shahar va viloyatlarda o‘qitishning ushbu shakliga mos korxona va tashkilotlarni aniqlash;
- ta’lim muassasasi va korxona o‘rtasida shartnoma imzolash;
- o‘rta darajadagi menejerlarga bo‘lgan ehtiyojlarni aniqlash;
- kadrlar tayyorlash uchun yo‘nalishni tashkil etish;
- kadrlar tayyorlash dasturlarini yaratish va ularni mehnat bozoridagi talabga muvofiq yangilash;
- dual ta'limdan o‘tgan xodimlarning malakasini baholash.

Qonun loyihasi dual ta’limni tashkil etish tartibi va uning shartlarini belgilaydi.

Masalan, dual ta'lim doirasida korxonaga yuborilgan talaba Mehnat kodeksiga muvofiq rasmiy ro‘yxatdan o‘tkazilishi taklif qilinmoqda.

Dual ta'limni tugatgandan so‘ng, talaba tashkilot bilan kelishilgan holda unda ishlashni davom ettirishi mumkin. Shu bilan birga, dual ta'limga talabalarni qabul qiluvchi tashkilot ularni ishga joylashtirishni kafolatlamaydi.

GERMANIYA Dual tizim mohiyatan ta'lim muassasasida va ishda parallel ravishda o‘qitishni anglatadi. O‘qitishning asosini nazariya va amaliyot o‘rtasidagi munosabatlar printsipi tashkil etadi.

Germaniyada ta'lim olishning dual modeli quyidagicha:

Ta'limning 70-80% ish joyida amalga oshiriladi;

Talaba haftada 3-4 kun korxonada va 1-2 kun kollejda o‘qiydi;

O‘quv rejalari: 1/3 umumiy ta'lim fanlari va 2/3 ixtisoslik fanlari;

O‘qish muddati 2 yildan 3,5 yilgacha o‘zgaradi;

Ta'limning asosiy xarajatlari korxona tomonidan qoplanadi.

Kasb-hunar ta'limining dual tizimining samaradorligi Ta'limning nazariy qismini takomillashtirish masalasi tug'iladi. Ishlab chiqarish mutaxassislari, muhandislar va professional ishchilar o‘zlarining pedagogik mahoratini sinovdan

o‘tkazishlari kerak. Shunday qilib, Rossiyada kasb-hunar ta'limi tizimi yaqin kelajakda ko‘plab islohotlarni boshdan kechiradi.

O‘zbekistonda yoshlarning kasblar va mutaxassisliklarni egallashga bo‘lgan qiziqishlarini qo‘llab-quvvatlash uchun keng imkoniyatlar yaratish maqsadida 2021/2022-o‘quv yilidan professional ta’lim tizimida dual ta’lim tashkil etiladi. Bu haqda 29-mart kuni Vazirlar Mahkamasining tegishli qarori qabul qilindi

Dual ta’lim ta’lim oluvchilar tomonidan zarur bilim, malaka va ko‘nikmalarni olishga qaratilgan bo‘lib, ularning nazariy qismi ta’lim tashkiloti negizida, amaliy qismi esa ta’lim oluvchining ish joyida amalga oshiriladi. Dual ta’limni tashkil etish tartibi O‘zbekiston Respublikasi Vazirlar Mahkamasi tomonidan belgilanadi.

**Dual ta’limni tashkil etish jarayonida tashkilotning vazifalari, huquqlari hamda majburiyatlari**

**Tashkilot vazifalari:**

professional ta’lim muassasasi bilan hamkorlikda dual ta’lim dasturini amalga oshirish bo‘yicha chora-tadbirlar rejasini belgilaydi;

professional ta’lim muassasasi bilan birgalikda o‘quvchilarni o‘qishga qabul qilish boshlanishidan kamida bir oy oldin dual ta’lim bo‘yicha tegishli shartnomalarni rasmiylashtiradi;

dual ta’limda o‘qitish muddatlarini hamda tashkilotga yuborilayotgan o‘quvchilar tarkibini professional ta’lim muassasasi bilan kelishadi;

o‘quvchilar bilan shartnomalar tuzadi va professional ta’lim muassasasi bilan kelishilgan muddatlarda o‘quvchilarni qabul qiladi;

har bir o‘quvchiga dual ta’lim dasturining ishlab chiqarish bilan bog‘liq amaliy qismini o‘rgatish uchun yuqori malakali mutaxassis ustozni biriktiradi;

biriktirilgan ustoz tomonidan dual ta’lim dasturi, lavozim yo‘riqnomalari va majburiyatlarning bajarilishini ta’minlaydi;

o‘quvchini o‘zlashtirgan kasb yoki mutaxassislik bo‘yicha natijalarini baholash jarayonini tashkil etadi;



o‘quvchining kasb yoki mutaxassisliklari bo‘yicha yakuniy davlat attestatsiyasida qatnashadi.

Tashkilot qonun hujjatlariga muvofiq boshqa vazifalarni ham bajarishi mumkin.

**Tashkilot quyidagi huquqlarga ega:**

mashg‘ulotlarning nazariy qismi o‘qitilishi yuzasidan professional ta’lim muassasasiga murojaat qilish;

dual ta’lim sifatini oshirish yuzasidan professional ta’lim muassasasiga takliflar berish;

normativ-huquqiy hujjatlarni takomillashtirish va ularning loyihalarini ishlab chiqish yuzasidan takliflar berish;

bir nechta professional ta’lim muassasalari bilan hamkorlik qilish.

Tashkilot qonun hujjatlariga muvofiq boshqa huquqlarga ham ega bo‘lishi mumkin.

**Tashkilot quyidagi majburiyatlarni o‘z zimmasiga oladi:**

mashg‘ulotlarning nazariy, o‘quv va amaliy qismini professional ta’lim muassasasida olib borish uchun sharoit yaratish;

o‘quvchilarni mehnat qonunchiligi asosida ishga qabul qilish;

o‘quvchilarni tashkilotda ishlab chiqarish bilan bog‘liq amaliy qismi davrida aniq ish joyi va zarur jihozlar bilan ta’minlash;

o‘quvchilarni tashkilot ustavi, ichki tartib-qoidalari, tibbiy (sanitariya), yong‘in xavfsizligi qoidalari hamda boshqa talablar bilan tanishtirish;

o‘quvchilarga o‘z ustaviga muvofiq amaliy jarayonlarda qatnashishga ruxsat berish;

o‘quvchilar kundaligi yuritilishini ta’minlash;

professional ta’lim muassasasi bilan birgalikda dual ta’lim amalga oshirganligi bo‘yicha hisobotlarni tayyorlash.

Tashkilot qonun hujjatlariga muvofiq boshqa majburiyatlarni ham bajarishi mumkin.

Masofaviy ta'lim – ishlab chiqarishdan ajralmagan holda, masofadan turib, axborot-kommunikatsiya texnologiyalari yordamida tahsil olish;

Dual ta'lim – ham kasbiy ta'limda o'qib, ham o'z yo'nalishiga mos ishda ishlash (shu yildan boshlab kollej va texnikumlarda joriy etiladi).

Masofaviy ta'lim an'anaviy ta'lim turidan quyidagi xarakterli xususiyatlari bilan farqlanadi.

Moslashuvchanlik – Ta'lim oluvchiga o'ziga qulay vaqt, joy va tezlikda ta'lim olish imkoniyati mavjudligi.

Modullilik – Bir biriga bog'liq bo'lmagan mustaqil o'quv kurslari to'plamidan - modullardan individual yoki guruh talabiga mos o'quv rejasini tuzish imkoniyati mavjudligi.

Parallellik – O'quv faoliyatini ish faoliyati bilan birga parellel ravishda, ya'ni ishlab chiqarishdan ajralmagan holda olib borish imkoniyati mavjudligi.

Keng qamrovlilik – Ko'p sonli o'quvchilarning bir vaqtning o'zida katta o'quv (elektron kutubxona, ma'lumotlar va bilimlar bazasi va boshqalar) zahiralariga murojaat qila olishi. Bu ko'p sonli o'quvchilarning kommunikatsiya vositalari yordamida o'zaro va o'qituvchi bilan muloqotda bo'lish imkoniyati.

Iqtisodiy tejamkorlik – O'quv maydonlari, texnika vositalari, transport vositalari va o'quv materiallaridan samarali foydalanish, o'quv materiallarini bir joyga yig'ish, ularni tartiblangan ko'rinishga keltirish va bu ma'lumotlarga ko'p sonli murojaatni tashkil qilib bera olish mutaxassislarni tayyorlash uchun ketadigan xarajatlarni kamaytiradi.

Ijtimoiy teng huquqlilik – Ta'lim oluvchining yashash joyi, sog'lig'i va moddiy ta'minlanish darajasidan qat'iy nazar hamma qatori teng huquqli ta'lim olish imkoniyati.

Internatsionallilik – Ta'lim sohasida erishilgan jahon standartlariga javob beradigan yutuqlarni import va eksport qilish imkoniyati.

O'qituvchining yangi roli – Masofaviy o'qitish o'qituvchining o'qitish jarayonidagi rolini yanada kengaytiradi va yangilaydi. Endi o'qituvchi o'zlashtirish



jarayonini muvofiqlashtirishi, yangiliklar va innovatsiyalarga mos ravishda berayotgan fanini muntazam mukammallashtirishi, saviya va ijodiy faoliyatini yanada chuqurlashtirishi talab etiladi.

Sifat – Masofaviy o'qitish usuli ta'lim berish sifati bo'yicha kunduzgi ta'lim turidan qolishmaydi. Balki, mahalliy va chet ellik dars beruvchi kadrlarni jalb qilib, eng yaxshi o'quv-metodik darsliklar va nazorat qiluvchi testlardan foydalangan holda o'quv jarayonini tashkil etish sifatini oshirishi mumkin.

Yuqoridagilarni hisobga olinganda masofaviy ta'lim kompleksi ancha qulayliklarga ega ekan. Lekin, nima uchun masofaviy ta'lim kerak bo'lib qoldi? – degan savol tug'ilishi tabiiy.

Bu savolga javob tariqasida quyidagilarni sanab o'tish mumkin:

- Ta'lim olishda yangi imkoniyatlar (ta'lim olishning arzonligi, vaqt va joyga bog'liqmasligi va boshqalar).
- Ta'lim maskanlariga talaba qabul qilish sonining cheklanganligi.
- Ta'lim olishni xohlovchilar sonining oshishi.
- Sifatli axborot texnologiyalarining paydo bo'lishi va rivojlanishi.
- Xalqaro integratsiyaning kuchayishi.

Yuqorida sanab o'tilgan sharoit va imkoniyatlar masofaviy o'qitishga ehtiyoj borligini ko'rsatadi. Umuman olganda masofaviy ta'limning *maqsad*iga quyidagilar kiradi:

1) Mamlakat miqyosidagi barcha hududlar va chet eldagi barcha o'quvchilar, talabalar, ta'lim olishni xohlovchilarga birdek ta'lim olish imkoniyatini yaratib berish.

2) Yetakchi universitetlar, akademiyalar, institutlar, tayyorlov markazlari, kadrlarni qayta tayyorlash muassasalari, malaka oshirish institutlari va boshqa ta'lim muassasalarining ilmiy va ta'lim berish potensiallaridan foydalanish evaziga ta'lim berishning sifat darajasini oshirish.

3) Asosiy ta'lim va asosiy ish faoliyati bilan parallel ravishda qo'shimcha ta'lim olish imkoniyatini yaratib berish.

4) Ta'lim oluvchilarni ta'lim olishga bo'lgan ehtiyojini qondirish va ta'lim muhitini kengaytirish.

5) Uzluksiz ta'lim imkoniyatlarini yaratish.

6) Ta'lim sifatini saqlagan holda yangi prinsipal ta'lim darajasini ta'minlash.

Yuqoridagilarni xulosa qilib shuni aytish mumkinki, masofaviy ta'lim kompleksini ta'lim muassasalariga joriy etilishi har tomonlama foyda keltiradi. Oliy ta'lim tizimida bu kompleksni joriy qilish uchun barcha shart-sharoitlar mavjud. Respublika miqyosidagi barcha Oliy ta'lim maskanlari (OTM) kompyuter, axborot va kommunikatsiya texnologiyalari bilan yaxshi ta'minlangan. Ularning barchasi Internet tarmog'iga ulanganlar. Ushbu texnologiyalarni ta'lim tizimiga keng joriy etish OTMlari oldiga qo'yilgan ko'p muammolarni o'z paytida xal etishga yordam beradi.

**Nazorat savollari**

1. Professional va Dual ta'lim tizimini farqlari haqida so'zlang.
2. Masofaviy dual ta'lim nima?
3. Ta'limda Ijtimoiy teng huquqlilikni izohlang.
4. Masofaviy ta'limning maqsadlarini izohlang.
5. Masofaviy ta'lim nima uchun kerak.

### 2.2. Elektron ta'limni tashkil qilish shakllari

Jahonning barcha oliy ta'lim muassasalarida oliy ta'lim sifati, ya'ni sifatli kadrlar tayyorlash hamma vaqt ham dolzarb masala bo'lib kelgan va shunday bo'lib qoladi. Sifat masalasi, ayniqsa, XX asrning oxiri va XXI asrning boshlarida yana ham muhim ahamiyat kasb etmoqda. Istiqlolning ilk kunlaridan boshlab yurtimizda ta'lim sohasiga yuksak e'tibor qaratilmoqda. Mamlakatimiz jahon hamjamiyatiga tobora keng kirib borayotgan bir sharoitda iqtisodiyotning turli tarmoqlarini modernizatsiyalash, jumladan, ta'lim jarayonida rivojlangan mamlakatlarning ilg'or tajribalaridan keng foydalanilmoqda.



Yevropada XVIII asr ohirida pochta aloqasining doimiy va foydalanish vujudga kelishi bilan, «muxbirli ta'lim» vujudga keldi. Pochta qatnashuvchilar o'quv materiallariga ega bo'ldilar, o'qituvchilar bilan muloqotda bo'ldilar va imtixonlar topshirishdi yoki ilmiy ish ko'rinishida topshiriqlar topshirdilar. Rossiyada bu uslub XIX asr oxirida vujudga keldi.

Onlayn o'qishning 4 turi. Har bir zamonaviy o'qituvchi bilishi kerak bo'lgan atamalar.

D-learning

Ingliz tilidan distance learning дистанционное обучение yoki masofaviy ta'lim- masofadan turib o'qishga imkon beradigan usul. Elektron ta'lim bilan chalkashtirmaslik kerak. Talaba real vaqtda o'qituvchi yoki boshqa talabalar bilan uchrashmaydi. Ammo shunga qaramay, ular orasidagi ikki tomonlama aloqa bo'lishi shart: elektron pochta, Skype.

E–learning

Bu ko'pincha o'quv kurslarni olib borish uchun tanlanadigan masofaviy o'qitish turlaridan biridir. O'quv mashg'ulotlari uchun talabaga Internet va kompyuter kerak bo'ladi. Siz uydan chiqmasdan seminarlarda, bitiruv kurslarida yoki hatto universitetda qatnashishingiz mumkin. Ko'plab kompaniyalar, trenerlar, universitetlar o'z xodimlari va talabalarini o'qitish uchun E–learning ni tanlaydilar. Elektron ta'lim kichik guruhlarda mashq qilish uchun ham, minglab guruhlarni o'qitish uchun ham mos keladi.

M-learning

Agar masofaviy o'qitish uchun barqaror Internet aloqasi bo'lgan mobil qurilma yoki noutbukdan foydalanilsa, demak bu M-learning ingliz tilida mobile learning bo'ladi.

B-learning

B-learning yoki blended learning - aralashgan ta'lim, an'anaviy va masofaviy o'qishni birlashtirishga imkon beradigan usul. Darsning maqsadlariga qarab, o'qituvchi bilan turli xil aloqa usullari qo'llaniladi. Agar mavzu amaliy ko'nikmalarni talab qilsa, talabalar tinglovchilar oldiga kelishadi. Shu bilan birga,

ma'lumotlarning bir qismi elektron pochta orqali yuboriladi yoki video ma'ruza shaklida joylashtiriladi. Vaqti-vaqti bilan talabalar seminarlarda yoki treninglarda o'qituvchi bilan onlayn ravishda uchrashadilar.

Ta'lim sohasidagi onlayn ta'lim haqida gap ketganda, bu model 2000-yillarning boshlariga qadar talabalar sinfda bo'lib, jarayonni boshqargan o'qituvchi bilan juda sodda bo'ldi. Jismoniy hozirlik hech qanday miyadan emas edi, va boshqa har qanday ta'lim turi eng yaxshi shubha ostiga qo'yildi. Keyin internet sodir bo'ldi, qolganlari esa tarixdir. E-learning – tez o'sib borayotgan sanoat, 1980-yillarga borib taqaladigan va hatto undan oldin (masofaviy ta'lim va televidenie kurslarida) kuzatib boradigan oqibatlar – ushbu kitobning keyingi qismida muhokama qilinadi.

Hozirgi vaqtda kompyuterlar va Internet uchun mos keluvchi elektron ta'lim echimlari mavjud bo'lib, u deyarli har bir joydan ta'limni osonlashtirish uchun yaxshi elektron ta'lim vositasiga ega. Texnologiya shu qadar rivojlanganki, jo'g'rofiy bo'shliq siz sinfdagidek his qilishingizga yordam beradigan vositalardan foydalanish bilan ko'payadi. E-learning video, slideshow, hujjat va PDF kabi har qanday formatda toshare materiallarini taqdim etadi. Veb-seminarlar o'tkazish (jonli onlayn kurslar) va suhbat va xabar forumlari orqali professor-o'qituvchilar bilan muloqot qilish ham foydalanuvchilar uchun mavjud bo'lgan imkoniyatdir.

### *Ommaviy onlayn ochiq kurslarining modellari*

Olib borilgan ilmiy-metodik tadqiqotlarning tahlili shuni ko'rsatadiki, ommaviy onlayn ochiq kurs (OOOK)lar juda yangi yo'nalish bo'lganligi sababli (ommaviy onlayn ochiq kurs termini 2008-yil birinchi bo'lib kiritildi) kam o'rganilgan, shunday bo'lsada o'rganilayotgan va tadqiq qilinayotgan muammoning nazariy va amaliy tomonlarining ayrim qirralari bilan xorijda D. Komer, S. Dauns, K. G. Skripkin, L. Breslow, D. E. Pritchard, J. DeBoer, A. McAuley, B. Stewart, G. Siemens, D. Cormier, L. Pappano, S. Mak, R. Williams, J. Mackness va D. Simenslar, respublikamizda ommaviy onlayn ochiq kurslardan



foydalangan holda o'quv jarayonini tashkillashtirish mavzusi bo'yicha maqola muallifi V. Hamidovlar tadqiqotlar olib borganlar.

Elektron ta'lim (ET) rivojlanishi ta'lim jarayoniga uning samarali tadbiq etilishi amaliyotini yanada kengaytirib, hozirgi zamon ta'lim paradigmasining rivojla-nishida asosiy vektorlarni belgilab beruvchi zamonaviy tendentsiyalar va mavjud jahon tajribasiga diqqat bilan nazar solish-ni talab etmoqda. Bular orasida so'nggi 2–3 yilda ET rivojlanishining eng istiqbolli yo'nalishlaridan biri — OOOKlarning shakllanishi bo'ldi, ularning asosida esa ommaviy va barchaga teng imkoniyatlar mavjud bo'lgan ta'lim g'oyasi yotadi. OOOK — bu ommaviy ochiq onlayn kurslar (ingliz. — Massive Open Online Course, MOOC) bo'lib, ular jahonning ko'plab universitetlari tomonidan Yer sharining istalgan nuqtasida bo'lgan har qanday insonga masofaviy texnologiyalar yordamida professor-o'qituvchilar va yuz minglab talabalar (kurs tinglovchilari)ga erkin muloqotni tashkil qilish imkoniyatini beruvchi akademik kurslarni taqdim etadi. OOOKning siri nimadan iborat? Nima uchun bunday noodatiy ta'lim turi ommalashib, shiddat bilan rivojlanib bormoqda? Ushbu savollarga javob berishga harakat qilib ko'ramiz. Tarixga nazar solsak, OOOK atamasi 2008-yilda AQShda paydo bo'lib, ammo hozirgi ta'lim OOOK yo'nalishiga 2011-yilda Stenford shahrida yaratilgan Coursera asos solgan va u dastlab AQSHning uchta yirik universitetlarning ochiq resurslarini birlashtirdi, 2012-yilda Time jurnali fikriga ko'ra, eng yaxshi ta'lim sayti bo'lgan. Cour-sera asoschilari Endryu Ng va Dafna Koller o'z loyihasini ommaviy onlayn o'qitish g'oyasida («bir dunyodan bir kurs») shakllantirib, barcha xohlovchilarga jahonning yetakchi universitetlari ma'ruzalarini tinglash imkoniyatini berdi.

Ommaviy onlayn ochiq kurslar (OOOK) butun dunyoda Massive Open Online Courses (MOOC) deb yuritiladi.

**Ommaviy (Massive)** so'zi katta auditoriyani o'z ichiga olishini bildiradi.

Ommaviy so'zi tizimda talabalar o'zaro cheksiz muloqot qilishlari mumkinligini ham bildiradi.

**Ochiq (Open)** deb atalishiga sabab bu tizimdan erkin, ochiq foydalanish mumkinligidir. Ba'zi tijorat firmalari faqat pullik tizimda faoliyat yuritsa ham, lekin ko'pchilik ma'lumotlar va o'quv jarayonlarini bepul tashkil qilish imkoniyati ham mavjud.

**Onlayn (On-line)** deyilishi o'z-o'zidan aniq, chunki barcha jarayonlar internet tarmog'ida real vaqtda amalga oshiriladi. Tizimni kompyuterga ko'chirib, avtonom tarzda ishlab bo'lmaydi.

**Kurs (Courses)** so'zi axborotlar ma'lum bir yo'nalish bo'yicha jamlanganligini, ular eng zamonaviy usulda pedagogika va kompyuter texnologiyalari yutuqlaridan foydalanib tashkil etilganligini anglatadi.

OOOK o'z rivojlanish tarixida quyidagi formatlarda amaliyotga joriy etilgan: xMOOCs, cMOOCs va quasi-MOOCs.

xMOOCs formati an'anaviy universitet modeliga mos keladi (Coursera, edX, Udacity). Bu format 2011 yilda joriy etilgan. Bun tizimda o'qituvchi juda tajribali bo'lishi talab etiladi va talaba iste'molchi sifatida tashkil qilingan. Ma'ruzalar 3-30 minutdan oshmaydi. O'qituvchi bilan to'g'ri va teskari muloqot tashkil qilinmagan (bahs-munozaralardan tashqari). Coursera va Udacity talabalarni ko'proq jonli uchrashuvlar o'tkazishga chorlaydi.

cMOOC formati pedagogik muloqot modeliga asoslanilgan. Bunda bilimlar tizimiga tarmoqdagi jarayon, tarmoqni tashkil qilish, ma'lumot qo'shish, olish va chiqish faoliyatlari sifatida qaraladi. Har bir talaba o'zicha texnologiyani tanlaydi, unga infrastrukturani tashkil qilishda administratorlar yordam berishadi.

quasi-MOOC formali tarmoqdagi o'qitish dasturlari sifatida joriy etilgan (Khan academy, OpenCourseWare MIT - OCW). Texnik jihatdan olib qaraganda bular kurslar emas, balki ma'lum masalani yechishga yo'naltirilgan resurslardir (masalan, algebra bo'yicha masalani yechish). Ulardan ba'zi xorijiy oliy o'quv yurtlarida kreditlar to'plashda foydalanishadi.

Yuzlab kollej va universitetlar ham o'quv materiallarini internetga barcha uchun bepul va ochiq qo'yish amaliyotini yo'lga qo'ydi. Bugunga kelib MIT va Stenford universiteti ushbu amaliyotni yangi bosqichga ko'tarishga qaror qildi.



Ular endi nafaqat kursda o'tiladigan materiallarni, balki darsning o'zini ham bepul taqdim etishmoqda.

Stenfordda dastlab "Sun'iy intellekt faniga kirish" (Introduction to Artificial

Intelligence) nomli bepul "onlayn" kurs tashkil etilgan. Bu kursga dunyoning 190 dan ortiq mamlakatidan jami 160 mingdan ziyod talaba yozilgan. Ko'ngillilar yordamida kurs materiallari qisqa muddat ichida dunyoning 44 tiliga tarjima ham qilingan. Ishtirokchilarning 23 ming nafari kurs materiallarini to'liq tamomlab, imtihonlardan muvaffaqiyatli o'tgan hamda ushbu kursni bitirganlik to'g'risidagi guvohnomaga ega bo'lishgan.

2012-yil Stenford universiteti yana beshta bepul "onlayn" kurslarini tashkil etdi. Ularda o'qiyotgan talabalarning soni yarim millionga yaqin.

Bu borada Massachusets texnologiya instituti ham faollik ko'rsatmoqda. O'quv yurti tashabbusi bilan internet orqali bepul darslar beradigan "MITx" nomli yangi notijorat tashkiloti tuzildi. "MITx" qoshida ochilgan birinchi kurs – "Sxemalar va Elektronika" darsida qatnashish uchun 100 mingdan ziyod talaba ro'yxatdan o'tgan. "MITx" internet sahifasida yozilishicha, ro'yxatga yozilganlarning kamida 20 ming nafari dars mashg'ulotlarida to'liq va faol ishtirok etishmoqda.

Prinston universiteti, Berklidagi Kaliforniya universiteti, Michigan An-Arbor hamda Pensilvaniya universitetlari ham hamkorlikda bepul "onlayn" kurslarini tashkil etmoqda. Ushbu kurslar "Coursera" deb nomlangan internet saytida jamlangan. "Coursera"dan kurslarni ularning nomlari va yo'nalishi bo'yicha yoki ularni taqdim etayotgan universitetlar bo'yicha qidirib topish mumkin.

Bepul darslarni taqdim etuvchi yana bir sayt "Udacity" bo'lib, u ham "Coursera" bilan birgalikda Stenford universiteti mutaxassislari tomonidan bunyod etilgan.

Nufuzli universitetlarning onlayn kurslari

Dunyoning nufuzli universitetlari taqdim etayotgan ushbu bepul "onlayn" kurslarining manzillari quyidagilar:

- Coursera.org – https://www.coursera.org/
- EdX – https://www.edx.org/
- Udemy – https://www.udemy.com/
- LinguaLeo – http://lingualeo.ru/
- busuu – http://www.busuu.com/enc/
- TED – http://www.ted.com

**Coursera.** Rasmiy sayti: www.coursera.org

Ushbu ingliz tilidagi loyiha har xil bilimlar bo'yicha kurs tizimlarini o'tkazadigan universitetlar bilan hamkorlik qiladi. Tinglovchilar faqatgina kurslarni o'qibgina qolmasdan, kursdoshlari bilan gaplasha oladilar, Coursera OOOK testlar va imtihonlar topshiradilar

**Khan akademiyasi.** Rasmiy sayti: https://www.khanacademy.org

MIT va Garvardni bitirgan qobiliyatli talaba Salmanxan boshqa shaharda yashaydigan kichkina amakivachchasiga matematika fanidan yordam berish uchun «YouTube» saytiga videodarslarni joylashtirgach, bu sayt tezda ommalashib, mashhur bo'lib ketgan. Endi Khan akademiyasi saytida har xil mavzudagi 42000 dan ortiq bepul mikroma'ruzalar bor. Ulardan ko'pchiligi rus tilida ham mavjud.

**EdX ta'lim platformasi** . Uni Garvard Universiteti hamda Massachusets texnologiya instituti birgalikda "barcha yoshdagilar va turli millat vakillari uchun tekin, internet orqali interfaol ta'lim olishlari uchun" notijoriy tashkilot sifatida tashkil qilishgan.

EdX da ingliz tilida Garvard Universiteti, MIT va yana Berkeley Kaliforniya Universitetlarida (hamda 2013-yildan Texas Universiteti ham qo'shilgan)o'rgatiladigan kurslardan bilim olish mumkin.

Hozircha maskur EdX platformasida kimyo, tibbiyot, informatika, fizikaga oid kurslar qo'yilgan.

**Intuit.** Rasmiy sayti: www.intuit.ru



Oliy ta'lim va ikkinchi oliy ta'limni olish imkoniyati mavjud bo'lgan, shuningdek, professional qayta tayyorlash va malakani oshirish imkoniyatlarini taqdim qila oladigan yirik Rossiya internet-universitetidir. To'liq o'qish pullik, ammo intuit saytida turli sohadagi: informatika, fizika, matematika, iqtisodiyot va falsafa bo'yicha 500 dan ortiq kurslarni bepul o'qish mumkin. Hozirgi kunda ko'pgina kurslar video darslar shaklida ham berilmoqda. Ta'lim kurslarini tugatib bepul elektron sertifikat olish imkoniyati ham mavjud.

***Elektron ta'limni tashkil etishda dasturiy ta'minot***

**ZOOM** - bu videotelefoniya dasturiy ta'minoti bo'lib, Zoom Video Communications tomonidan ishlab chiqilgan. Bepul reja, bir vaqtning o'zida 100 ishtirokchiga 40 daqiqalik vaqt cheklovi bilan video-chat xizmatini taqdim etadi. Foydalanuvchilar pullik rejaga obuna bo'lish orqali yangilash imkoniyatiga ega. Eng yuqori reja 30 soatgacha davom etadigan uchrashuvlarda bir vaqtning o'zida 1000 ishtirokchini qo'llab-quvvatlaydi.

COVID-19 pandemiyasi paytida masofadan turib ishlash, masofadan turib o'qitish, va Internetdagi ijtimoiy aloqalar uchun Zoom-dan foydalanish sezilarli darajada ko'paygan. Ushbu o'sish Zoom-ni 2020 yilda 477 million marta yuklab olingan holda dunyo bo'ylab eng ko'p yuklab olingan 5-o'rinni egallashiga olib keldi.

Zoom dastlab 2011 yilda tashkil etilgan. Zoomning beta-versiyasi, unda 15 tagacha video ishtirokchilar ishtirokida konferentsiyalar o'tkazilishi mumkin edi, 2012 yil 21 avgustda ishga tushirildi.2013 yil 25-yanvarda dasturning 1.0-versiyasi chiqarilib, har bir konferentsiya ishtirokchilari sonining 25 taga ko'payishi kuzatildi. Birinchi oyning oxiriga kelib Zoom-ning 400 ming foydalanuvchisi bor edi, ular 2013 yil may oyida 1 millionga yetdi. COVID-19 pandemiyasi boshlangandan so'ng, 2020 yil fevraliga kelib, Zoom 2020 yilda 2,22 million foydalanuvchiga ega bo'ldi - bu 2019 yilga kelib butun foydalanuvchilar sonidan ko'p bo'lgan aksiya narxi 35 foizga ko'tarilgan. 2020 yil mart oyining bir kunida

Zoom dasturi 2,13 million marta yuklab olindi 2020 yil aprel oyida Zoomda 300 milliondan ortiq kunlik yig'ilish qatnashchilari bor edi.

**Google Meet**

Google bilan tanishish Google Hangouts -ning yuqori versiyasidir.

Yaqin vaqtgacha Hangouts -ning bepul versiyasi bo'lgan, bir vaqtning o'zida bir nechta odamlarning video uchrashuvini (250 tagacha) qo'llab - quvvatlaydigan Meet, Google Workspace platformasiga (sobiq Google Suite) obuna bo'lishni talab qilgan, barcha maktablarda allaqachon Google Classroom mavjud.

2020 yil may oyidan boshlab Google Meet hamma uchun bepul bo'lishini e'lon qildi va oddiy Google hisobidan videokonferentsiyalar yaratish uchun cheklovlarsiz foydalanish kifoya. Bundan tashqari, Meet ham Gmail bilan birlashtirilgan, shuning uchun siz videokonferentsiyani darhol boshlash tugmachasining chap pastki qismidagi Uchrashuv qutisini ko'rishingiz mumkin. Shu sababli, Hangout tez orada bekor qilinadi va uning o'rnini Meet egallaydi.

Google Meet -ga turli yo'llar bilan kirish mumkin: Saytdan meet.google.com/

Meet ilovasidan Android yoki iPhone uchun.

Saytda ham, ilovada ham, yangi uchrashuvlar yaratish yoki mashg'ulotlarni boshlash yoki qo'shilish uchun, siz Google hisobingiz yoki kompaniyangiz yoki maktabingiz tayinlagan hisob bilan kirishingiz kerak (Classroom orqali). Siz ham mumkin hisobni ishlatmasdan videokonferentsiyaga qo'shiling Agar sizda uchrashuv kodi bo'lsa.

Esda tutingki, Google Meet yoki boshqa Google xizmatlarini ochganingizda hisobni o'zgartirish o'ng yuqori burchakdagi profil belgisini bosish orqali amalga oshiriladi. Shunday qilib, agar Meet sayti uchrashuvni boshlamasdan ochilsa, hisobni o'zgartirish va Classroom yoki Google Workspace -da ro'yxatdan o'tgan xizmatga kirish uchun yuqori o'ng burchakdagi profil belgisini bosing.

**Nazorat savollari:**

1. OOOK qisqartmasini izohlab bering.



2. OOOK ning rivojlanish tarixida qanday formatlar bo'lgan?
3. xMOOC formatini izohlab bering.
4. cMOOC formatini izohlab bering.
5. quasi-MOOC formatini izohlab bering.
6. MOOK dastlab qaysi universitetlarda paydo bo'lgan?
7. Ommaviy onlayn ochiq kurslarga misollar keltiring.
8. Coursera, Khanacademy va EdX OOOK larini izohlang.
9. Intuit va Яndex maktabi OOOK larini izohlang.

### 2.3. Elektron ta'limni tashkil qilish usullari. Smart texnologiyalari

Masofaviy o'qitish uslubi asosida tinglovchilarni o'qitish hozirgi kunning eng rivojlanib borayotgan yo'nalishlaridan bo'lib, o'qituvchi bilan tinglovchilar ma'lum bir masofada joylashgan holda ta'lim berish tizimidir. O'qituvchi va tinglovchining ma'lum bir masofada joylashganligi, o'qituvchini dars jarayonida kompyuterlar, sputnik aloqasi, kabel televidenyasi kabi vositalar asosida o'quv ishlarini tashkil qilishini talab qiladi. Zamonaviy kompyuter texnologiyalarining tez rivojlanib borishi, ayniqsa, axborotlarni uzatish kanallarining rivojlanishi telekommunikatsiya sohasiga o'ziga xos tarixiy o'zgarishlar kiritmoqda.

Masofaviy o'qitish quyidagi texnologiyalarni o'z ichiga oladi:

**Interaktiv texnologiyalar:**

audiokonferentsiyalar;

videokonferentsiyalar;

ish stolidagi videokonferensiyalar;

elektron konferentsiyalar;

ovoz kommunikatsiyalari;

ikki tomonlama sputnik aloqa;

virtual borliq.

**Nointeraktiv texnologiyalar:**

bosib chiqarilgan materiallar;

audiokassetalar;

videokassetalar;

bir tomonlama sputnik aloqa;

televizion va radio ko'rsatuvlari;

disketa va CD-ROMlar.

### *Virtual borliq texnologiyasi*

Informatika va axborot texnologiyalari yo'nalishida virtual tushunchasi keng ma'noda qo'llanilmoqda. Masalan: virtual mashina, virtual xotira, virtual disk, virtual aloqa, virtual sayohat, virtual sinf va h.k.

Birgina ushbu sohasida ham virtual tushunchasi turli shakl va ma'nolarda qo'llanilib kelinmoqda va bir-biridan farqli ma'nolarni anglatadi. Masalan, multimedia tizimlarida virtual tushinchasi virtual borliq ma'nosini beradi.

Virtual (lotincha Virtualis — mumkin bo'lgan, ya'ni muayyan bir sharoitlarda sodir bo'ladigan yoki ro'y berishi mumkin bo'lgan) tushunchasi narsalar va hodisalarning vaqt va makonda mavjud bo'lmagan, lekin ob'yektiv narsalar yoki sub'yektiv obrazlarning amalga oshish ehtimoli mavjud bo'lgan jarayonni anglatadi.

«Virtual borliq» atamasi 1970 yillarning oxirida Massachuset texnologiya institutida Jaron Lanier tomonidan o'ylab topilgan. U 1984 yilda dunyoda birinchi virtual borliq firmasini tashkil etdi. Bu atama kompyuterda yaratiladigan muhitda insonning mavjudligi g'oyasini ifoda etadi. «Virtual borliq» atamasi muomalaga amerikalik kinematografchilar tomonidan kiritilgan. Ular muayyan sabablarga ko'ra tabiiy yo'l bilan amalga oshirib bo'lmaydigan xayoliy imkoniyatlarni belgili-grafik shaklda sun'iy amalga oshirish mumkinligi haqidagi kinolentani shu nom bilan chiqarganlar.

Virtual borliq — inson real borliqda harakat qilayotgani illyuziyasini kompyuterda yaratish imkonini beruvchi interfaol texnologiya. Bunda ob'yektiv borliqni tabiiy sezgi organlari yordamida idrok etish o'rnini maxsus interfeys, kompyuter grafikasi va ovoz vositasida sun'iy yaratilgan kompyuter axboroti egallaydi. Virtual borliq amalda yo'q narsa, uni qo'l bilan tutish, uning ta'mi va hidini his qilish mumkin emas. Shunga qaramay, u mavjud va inson bu xayoliy olamga kirib, uni nafaqat kuzatadi va boshdan kechiradi, balki unga ta'sir



ko'rsatish imkoniyatiga ham ega bo'ladi, ushbu olamda mustaqil harakat qiladi, uni o'zgartira oladi. Virtual olam — inson borlig'ining o'ziga xos shakli va odamlar ma'naviy aloqasining alohida madaniy ifodasidir.

Ammo virtual borliq real fizik borliqdek lazzat baxsh eta olmaydi, chunki bu borliq ta'sirida vujudga keluvchi his-tuyg'ular ko'p jihatdan uning o'zi bilan emas, balki uni biz qanday idrok etishimiz bilan belgilanadi. Biz virtual dengizda cho'milishimiz mumkin, ammo bunda paydo bo'luvchi histuyg'ularimiz bu dengizni biz qanday idrok etishimizga bog'liq bo'ladi.

Virtual tarvuz haqiqiy tarvuzdan shirin emas va h.k. Virtual borliqni odamlar yaratadi. Shu bois virtual borliqda mavjud barcha narsalarning manbai inson ongidir. Binobarin, virtual borliq ong, ong osti sohasi va fantaziya chig'irig'idan o'tuvchi fizik borliqdan shakllanadi. Virtual borliq ob'yektiv tarzda, ya'ni inson miyasida emas, balki kompyuterda mavjud bo'ladi. Ayni vaqtda, u inson ongining mahsulidir. Inson tomonidan yaratilganidan keyin u inson ongidan qat'iy nazar yashashda davom etadi, bu ongga har xil ta'sir ko'rsatadi, mazkur ongning mazmuniga - bilimlar,emosiyalar, kayfiyat hamda ongning boshqa unsurlariga qarab, har xil idrok etiladi.

Bugungi kunda virtual borliq inson madaniy faoliyatining turli sohalarida qo'llanilmoqda. Virtual borliqdan eng avvalo u vujudga kelgan sohada, fanda, jumladan fizikada suyuqlik va gazlar dinamikasini modellashtirishda, kimyoda kimyoviy reaksiyalar modelini tuzishda, geologiya va geografiya fanlarida foydalanilmoqda.

Muhandislik sohasida, ayniqsa, xavfli sharoitlarda: ochiq kosmosda, dengiz va okeanlarning chuqur joylarida, yadro muhandisligida robotlarni masofadan turib boshqarishda virtual borliq keng qo'llanilmoqda.

Kompyuter dizayni va uning ajralmas hamrohi - kompyuter ishlab chiqarishi raketalar va samolyotlar, avtomobillar katta binolar konstruksiyalarini sinovdan o'tkazishda yagona jarayonga birlashtirildi.

Virtual borliq texnologiyasidan harbiylar ham keng foydalanmoqdalar. Masalan, AQSH armiyasida harbiy xizmatchilarda merganlik ko'nikmalarini

shakllantirishda imitatorlardan, jang sharoitida tez va to‘g‘ri qarorlar qabul qilish ko‘nikmasini shakllantirish uchun esa harbiy doktorlardan foydalaniladi. Juda qimmatga tushadigan va atrof muhitga katta zarar yetkazadigan harbiy mashqlar imitasiya qilinmoqda. Tank qismlarida tankdan o‘q uzishni hamda tank jangida askarlar va ofiserlarning shaxsiy ishtirokini imitasiya qiluvchi harbiy o‘yinlardan foydalanilmoqda.

Loyihalashtirilgan, lekin hali yasalmagan qurol-aslaha turlari sinovdan o‘tkazilmoqda. Harbiylar olingan ma’lumotlarni tahlil qilish va ularga baho berish uchun ham kompyuter imitasiyasidan foydalanmoqdalar. Ta’lim sohasida mashq trenajyorlarini yaratishda virtual borliq texnologiyasidan foydalanilmoqda. Yaqinda virtual kutubxonalar va muzeylar tashkil etish konsepsiyasi taklif qilindi. Masalan, virtual kutubxonalarda foydalanuvchi kompyuter yordamida kitob javonlarining vizual tasviri bo‘ylab harakatlanishi, kerakli adabiyotlarni topishi va olib ko‘zdan kechirishi, zarur holda esa ulardan nusxa ko‘chirishi mumkin. Virtual muzey konsepsiyasi bir qadar boshqacha. Virtual muzey foydalanuvchilarga kolleksiyadagi istalgan eksponatni uning tabiiy, uch o‘lchovli ko‘rinishida ko‘rish imkonini beradi. Ammo bu tasviriy yechish qobiliyati ancha yuqori bo‘lgan displeylarni taqozo etadi. Shunday qilib, virtual borliq nazariy izlanishlardan ommaviy axborot vositalari va telekommunikasiyalar ajralmas qismi bo‘lgan hozirgi zamon madaniyatining tarkibiy qismiga aylandi.

Virtual borliq – bu sun’iy hosil qilinadigan axborot muhiti bo‘lib, u atrof-muhitni odatiy usulda tasavvurni turli texnik vositalar asosida hosil qilinadigan axborotlar bilan almashtirishga qaratiladi. Ta’limiy maqsadlarda virtual reallik vositalarini ishlab chiqishga qaratilgan axborotlarni vizuallashtirish vositalarini yaratish boshqa texnik vositalar yordamida erishib bo‘lmaydigan pedagogik samarani berishi mumkin.

Virtual borliq immersivlik va interfaollik tushunchalari bilan bog‘liq.

Immersivlik deganda odamning virtual borliqda o‘zini faraz qilishini tushunish lozim.



Interfaollik foydalanuvchi real vaqtda virtual borliqdagi ob’yektlar bilan o‘zaro muloqotda bo‘lib ularga ta’sir ko‘rsatishga ega bo‘ladi.

Virtual borliq turlari:

- Passiv virtual borliq (passive virtual reality) - inson tomonidan boshqarilmaydigan avtonom grafik tasvirni tovush bilan kuzatilishi;
- Tekshiriluvchi virtual borliq chegaralangan miqdorda foydalanuvchiga taqdim qilinadigan ssenariy, tasvir, tovushni tanlash imkonining borligi;
- Interfaol virtual borliq treking vazifasini bajara oladigan maxsus qurilma yordamida yaratilgan dunyo qonunlari asosida virtual muhitni foydalanuvchi o‘zi boshqara olishidir;

Treking virtual muhitdagi real ob’yektning joylashishi koordinatalarini (x, y, z) va uni fazoda joylashishi burchaklarini (a, b, g) berishga mo‘ljallangan.

Virtual borliq tizimi deganda – biz imitasion dasturiy va texnik vositalarni qabul qilamiz. Interfaollikni ta’minlash uchun, virtual tizim boshqaruvchi amallarni qabul qilishi kerak. Bu amallar ko‘pmodallikga, ya’ni ko‘z bilan ko‘radigan, tovush orqali qabul qiladigan bo‘lishi kerak. Bu amallarni amaliyotda bajarish uchun zamonaviy tizimlarda turli tovush va videotexnologiyalardan foydalaniladi. Masalan, katta hajmli tovush va videotizimlari, shuningdek odamning bosh qismiga o‘rnatiladigan shlem va ko‘zoynak displeylar, “hid sezadigan” sichqonchalar, boshqaruvchi qo‘lqoplar, kibernetik nimchalar simsiz interfeys birgaligida ishlatiladi.

Vitual borliqning insoniyat uchun ta’siri:

- inson hayotini tashkil qilishda va tartibga solishda;
- insonlar o‘rtasidagi aloqaning yangi shakli;
- hayotning asosiy sohalari siyosat, iqtisod, san’at va turizm sohalariga ijobiy ta’siri borligi;
- virtual olam bilan inson o‘zining tartib qoidalari va o‘z muhitini yaratish mumkinligi;
- hayot va virtual borliq o‘rtasidagi aldanish mavjudligi.

Vitual borliqning rivojlanishida uch o'lchovli muhit va internet texnologiyalarining imkoniyatlarining rivojlanganligi katta ta'sir o'tkazdi. Natijada, turli sohalarda virtual reallik ishlatila boshladi.

Masalan:

- kino olamida 1982 yil yaratilgan TRON nomli rasmli film, bu sohadagi katta qadam bo'ldi. Hozirgi vaqtda virtual realliksiz bu sohani tasavvvur qilish qiyin.

- 2009 yil BBS radiosi tomonidan yaratilgan virtual drama bu sohada ham kelajagi bor ekanligini anglatmoqda;

- san'at sohasida 1970 yil David Em o'zining birinchi virtual ko'rgazmasi bilan ushbu atamani imkoniyatlarini ochib bergan;

- musiqa sohasida ham elektron musiqa asboblari virtual reallik imkoniyatlaring mahsulidir.

Virtual reallikning yaratishda axborot texnologiyalarining kompyuter grafikasi, real vaqt rejimi va dasturlash texnologiyalarisiz shakllantirib bo'lmaydi. Bunda hozirda kompyuter grafikasining OpenGL, Direct3D, Java3D, va VRML kutubxonalaridan, dasturlashdan esa, C++, Perl, Java va Python tillaridan foydalanilmoqda.

Hozirgi kunda turizm sohasida virtual reallikning qo'llanilishi natijasija virtual sayohat tushunchasi paydo bo'ldi. Virtual sayohat – multimedia ilovalari asosida simulyasilangan sayohat turidir. Bunda multimedia ilovalari sifatida matn, rasm, tovush, panorama, animasiya va video vositalari ishtirok etishi mumkin. Birinchi virtual sayohat 1994 yil Dublay qasrida qirolicha Yelizabeta 2 tomonidan tashkillashtirilgan.

Virtual borliqni hozirda internet texnologiyalarisiz tasavvur etish qiyin. Internet – XX asr mo'jizasi. Kim orqada qolib ketsa, keyin virtual dunyo taraqqiyotiga yetolmaydi. Internet – insoniyat qabul qilishining yangi o'lchami. Uni egallash bir tomondan oson, ikkinchi tomondan murakkab. Uning osonligi shundaki, dasturlarning eng osoni oddiy brauzerdan (hammma kompyuterda mavjud bo'lgan "Internet Explorer" brauzerdan) foydalanishni bilsangiz kifoya.



Internetni barcha xizmatlaridan foydalanish uchun bu dastur yetarli. Buning uchun, birinchidan, Internet xizmatlaridan foydalanish bo'yicha bilim va malaka talab qilinadi, ikkinchidan, tarmoqdagi xizmat va ma'lumotlar asosan xorijiy tillarda berilgan. O'zbek tilida joriy qilingan xizmatlar, nashr qilingan ma'lumotlar hozircha ko'p emas.

Mavjud hayotdagi bor narsalar Internetda – umumjahon kompyuter tarmog'ida ham mujassam.

Uni mukammal egallasangiz:

- xat yozib, javobini soniyalarda olasiz;
- tanishib, davra suhbatlar qurasiz, seminar, konferensiyalarda qatnashasiz;
- sirtqi o'quv yurtlarda ta'lim olasiz;til o'rganib, xorijiy matnlarni tarjima qilasiz, lug'atlardan foydalanasiz; ajoyib umumjahon ensiklopediyalaridan foydalanasiz;
- kitob, gazeta va boshqalarni o'qiysiz, uyingizda dunyo kutubxonasi bo'ladi;
- uyingizda o'tirib biznes va ijod bilan shug'ullanasiz;
- pulli va pulsiz amallar bajarasiz;
- dunyoga sayohat qilasiz;
- virtual (xayoliy) hayotga kirasiz va hokazo.

Xullas, Internetda ham hayotdagidek barcha voqea va hodisalarda real va virtual ishtirok etishingiz mumkin.

Vitual borliq deb real dunyoni kompyuter simulyasiyasi orqali yaratilgan muhitiga aytiladi. Vitual borliqning asosiy 3 ta xususiyati mavjud. Ular:

- ta'sir doirasining kengligi;
- yuqori vizuallashganligi;
- uch o'lchovli muhit.

***Smart texnologiyalari tushunchasi***

SMART-ta'limning keng tarqalishi birinchi navbatda Internet-texnologiyalarni takomillashtirish bilan, ikkinchidan, Wi-Fi, 3G, 4G kabi simsiz

texnologiyalarning rivojlanishi va uchinchidan, Internetda onlayn ta'lim resurslarining keng tarqalganligi bilan bog'liq.

SMART ta'limning asoslarini shakllanishida, shuningdek, Facebook, YouTube, Twitter va turli bloglar kabi, odamlarning o'z Internet-kontentini yaratishga imkon beradigan Web 2.0 texnologiyalarining rivojlanishi xizmat qildi.

Ta'lim dasturlarida Web 2.0 texnologiyalarining imkoniyatlarini qanday qo'llash mumkin?

Ushbu savolga bir qator javoblar mavjud:

o'quv materiallarini bepul tarqatish uchun tarmoqli jamoalardan foydalanish;

mustaqil o'quv materiallarini yaratish;

informatika sohasida maxsus bilim va ko'nikmalarsiz faoliyatning yangi shakllariga qatnashish.

O'qituvchilar ushbu texnologiyalarni bir-biri bilan va o'quvchilarining ota-onalari bilan muloqotda bo'lishlari, kasbiy tajriba almashishlari, mashg'ulotlarning mazmunini yangi materiallar bilan boyitish, o'quvchilarning o'qishga bo'lgan qiziqishini oshirish, kasbiy rivojlanish uchun foydalanishlari mumkin. O'qituvchi va o'quvchilar ta'lim jarayonida teng ishtirokchilarga aylanishadi: ularning har biri zarur ma'lumotlarga ega bo'lish imkoniyatiga ega bo'lishadi, umumiy tadqiqotning xulosasini har biri o'z ishi natijalari bilan to'ldiradi.

Microsoft Power Point yoki Macromedia Flash singari dasturiy ta'minot paketlaridagi multimediya prezentatsiyalaridan foydalangan holda o'quv mashg'ulotlarini o'tkazish me'yoriga aylandi. Ammo odatiy taqdimot texnologiyalari (Microsoft Power Point, Macromedia Flash) bilan bir qatorda taqdimotning slayd-shou ko'rinishidan voz kechish imkonini beradigan interfaol texnologiyalar deb nomlangan vositalar paydo bo'ldi.

Interaktiv jihoz, masalan SMART Boards interaktiv doskasi yordamida axborotlarni uzatishda ma'ruzachiga quyidagi imkoniyatlarni yaratadi: maxsus rangli markerlar bilan yozish, o'quv materialini namoyish qilish, ekrandagi tasvir ustiga yozma sharh berish mumkin. Shu bilan birga, SMART Boards interaktiv



doskasida yozilgan hamma narsalarni o'quvchilarga berilishi, ma'lumotlarni saqlashning turli vositalarda saqlanishi, chop etilishi, darsda qatnashmagan o'quvchilar elektron pochtasiga yuborilishi mumkin. SMART Boards interaktiv doskasida ma'ruza davomida yaratilgan o'quv materiallari doska ichida o'rnatilgan video yozuvchi moslama yordamida yozib olinishi, saqlanishi va qayta-qayta namoyish etilishi mumkin.

Doskaning interaktivligini ta'minlaydigan bir nechta texnologiyalar mavjud. Bu texnologiyalardan biri sensorli rezistorli, boshqasi - SMART Technologies kompaniyasining DVIT texnologiyasidir. Ularda ekranning burchaklarida shinatiladigan maxsus raqamli video kameralardan foydalaniladi. Bundan tashqari, maxsus moslama yordamida har qanday plazmali panellarni interaktiv doskaga aylantirish mumkin.

SynchronEyes dasturiy paketi yordamida, o'qituvchi o'quvchilarning nima bilan shug'ullanishini kuzatishi, o'quvchilar ishlayotgan barcha monitorlarni ko'rsatishi, o'quvchilar monitorlarini bloklashi, interfaol doskadan barcha kompyuterlarga ma'lumotlarni, masalan, test materiallarini jo'natishi mumkin.

Interaktiv doskalarda ishlashda o'quvchilar diqqatini yig'ish yaxshilanadi, o'quv materiallari tez o'zlashtiriladi va natijada har bir talabaning fanlardan o'zlashtirishi oshadi.

Smart Classroom Suite - interaktiv o'rganish uchun mo'ljallangan dastur. Smart Classroom Suite interaktiv o'quv dasturi kompyuterlashtirilgan sinflarda o'qituvchilar va o'quvchilar uchun mo'ljallangan maxsus dasturiy paket hisoblanadi. Ushbu paket

Smart Notebook™ hamkorlikda ta'lim olish dasturiy ta'minoti;

Smart Notebook™ CE o'quvchilar uchun dasturiy ta'minot,

Smart Sync™ sinfni boshqarish dasturiy ta'minoti;

Smart Response™ interaktik so'rovlarni amalga oshirish dasturiy ta'minotlarini o'z ichiga oladi.

Smart Classroom Suite dasturi bilan o'qituvchilar sinfda o'rganish jarayonini samarali boshqarishlari va darslarni o'tkazishlari mumkin. Foydalanish

oson bo'lgan vositalar o'qituvchilarga qiziqarli multimedia darslarini tayyorlashga yordam beradi. Asboblar panelini ishlatish orqali o'qituvchilar bir tegish bilan Smart Exchange™ veb-saytiga boshqa o'qituvchilar tomonidan yaratilgan darslarni topishlari yoki o'z tajribalarini boshqalar bilan baham ko'rishlari mumkin.

Zamonaviy ta'limga yangi yondashuvlarni turli kichik dasturiy ta'minotlar (gadjetlar) siz tasavvur qilish qiyin. Gadjetdan SMART o'rganish vositasini yaratish uchun qo'shimcha dasturiy ta'minotni o'rnatishingiz kerak. Smartfon yoki planshetga qanday dasturiy ta'minotni o'rnatish kerak? Buni qanday qilish kerak?

Ushbu masalalarni hal qilish uchun Google tizimi mobil qurilmaga SMART ilovasini o'rnatadigan «Play Market» ilovasini taklif qiladi.

«Play Market» mobil operatsion tizimi Android smartfonlari va planshetlarining standart vositalarida o'rnatilgan ilovadir. Ushbu ilovadan foydalanish uchun Google da ro'yxatdan o'tishingiz va hisobingizni (akkauntingizni) rasmiylashtirishingiz kerak. Ro'yxatdan o'tgan foydalanuvchilar Google tizimining barcha tarmoq dasturlariga kirish huquqiga ega bo'ladilar. Dastur foydalanuvchi uchun hordiq va mashg'ulot uchun juda ko'p toifadagi ilovalarni taqdim qiladi.

Har bir o'quv fani uchun juda ko'p sonli ilovalar mavjud. Misol uchun, Google Play Market ga bitta o'vuv fani qidiruvi nomini kiritishning o'zi kifoya va monitorga ingliz tili va rus tili mobil ilovalari, adabiyot, matematika, algebra, geometriya, fizika, kimyo, biologiya, jismoniy tarbiya fanlari bo'yicha topilgan ilovalar ro'yxati chiqadi.

Fanlarni o'rganish uchun kerak bo'ladigan ba'zi mobil ilovalardan namunalarini ko'rib chiqamiz.

"Matematik topqirlik" og'zaki hisob-kitob qobiliyatini o'stirish ilovasi. Ilova tez hisoblash uchun mavjud algoritmlarni aks ettiradi. Har bir o'quvchi ularni o'rganishi mumkin, so'ngra nazariy bilimlarni amaliy mashqlarda mustahkamlashi, shu tariqa og'zaki hisoblash amaliy tajribalarini boyitishi mumkin. Bu ilovani



yaratuvchilari og'zaki hisobda tarmoqdagi boshqa foydalanuvchilar bilan raqobat qilish imkonini ham hisobga olishgan.

«GeoGebra» dasturi barcha darajalarda matematikani o'rganish uchun mo'ljallangan dastur hisoblanadi. Unda geometriya, algebra, statistika va boshqa ko'plab qo'llanmalarni topishingiz mumkin.

«Chemist» ("Kimyochi") dasturi kimyo darslariga qo'shimchalar. Dastur virtual laboratoriya sifatida amalga oshiriladi. Bu erda har bir kishi "professor" sifatida eng ajoyib tajribalarni o'tkazishi mumkin. Dastur yuqori sifatli 3D va detallar bilan ta'minlangan. "Laboratoriya" omborxonasida ikki yuzga yaqin kimyoviy elementlar mavjud.

«Molecules» ("Molekulyar") dasturi bilan o'quvchilar turli moddalar bo'yicha yangi bilimlarga ega bo'lishlari mumkin. Ilovada ko'plab molekulyar modellar mavjud. Har bir molekula va molekulyar tuzilmalar va moddalar haqida to'liq ma'lumot topish mumkin.

«Anatomy 3D Pro» ("Anatomiya 3D") ilovasi. Ushbu dastur bilan o'quvchilar inson tanasining ichiga kiradilar. Dastur 3D formatdagi barcha nozikliklarning noyob detallari bilan tavsiflanadi. Dastur tezkor qidiruv funktsiyasi bilan ta'minlangan. O'z bilimingizni tekshirish uchun qiziqarli viktorina taklif etiladi.

«Star Walk 2» ilovasi yulduz osmonni o'rganish uchun mo'ljallangan. Unda o'quvchilar barcha yulduzlar va galaktikalar nomini va manzilini ko'rishlari, shuningdek, ular haqida ma'lumot olishlari mumkin. Shuningdek, yulduzlar turkumi va ularning tarixi ham bor.

«Edmodo» ("Edmodo") ilovasi - o'qituvchilar va o'quvchilar uchun ta'lim jarayoniga yordam beradi uchrashuv joyi. Dasturning maqsadi - o'qituvchilar va ta'lim olayotganlarga vaqt va manzilidan qat'iy nazar doimiy ravishda o'zaro aloqa qilish, bog'lanish imkoniyatini ta'minlash.

«Plickers» ("Plickers2) dasturi sizga mobil telefondan foydalanib, o'quvchilar bilan so'rovlarni o'tkazishga imkon beradi. Uning asosini mobil ilovalar, sayt va QR (Quick Response, ya'ni tezkor javob) - kodlari bilan bosilgan

kartachalari tashkil qiladi. «Plickers» dasturi bolalarning bilimlarini muntazam monitoringini amalga oshirishga imkon beradi, bu darsdan bir necha daqiqadan ko'proq vaqt talab qiladi.

**Nazorat savollari**

1. Interaktiv texnologiyalar va Nointeraktiv texnologiyalar haqida so'zlab bering.
2. Virtual borliq texnologiyasi tushunchasini izohlang.
3. Virtual borliq turlarini izohlang.
4. Virtual borliq tizimi deganda nimani tushunasiz?
5. Vitual borliqning insoniyat uchun ta'siri.
6. Smart texnologiyalari tushunchasini izohlang.

### 2.4. Imkoniyati cheklanganlar ta'limi uchun elektron pedagogika

Xalq ta'limi tizimida turli ehtiyojga ega bo'lgan bolalarga qaratilgan muassasalar — o'qitish darajasi ta'lim standartlaridan yuqori bo'lgan muassasalar (ixtisoslashtirilgan muassasalar) va imkoniyati cheklangan bolalar uchun ta'lim muassasalari faoliyat yuritadi. (O'zbekiston Respublikasi Prezidentining Farmoni, 29.04.2019 yildagi PF-5712-son)

**Imkoniyati cheklangan bolalarga ko'rsatiladigan ta'lim xizmatlari sifatini yaxshilash**:

imkoniyati cheklangan bolalar ta'lim oladigan ta'lim muassasalari binolariga qo'yiladigan talablarni ishlab chiqish va tasdiqlash;

imkoniyati cheklangan bolalar o'qitiladigan ta'lim muassasalarini zarur adabiyotlar, metodik qo'llanmalar, turli kasblarga o'qitish uchun bo'ladigan uskuna va jihozlar bilan ta'minlashga qaratilgan chora-tadbirlarni amalga oshirish;

imkoniyati cheklangan bolalarni o'qitish uchun inklyuziv ta'lim tizimini tashkil etish, umumta'lim muassasalarini maxsus moslamalar (ko'tarish qurilmasi, pandus, tutqich, boshqalar), shuningdek tegishli kadrlar (pedagog-defektolog, bolalarni ruhiy-pedagogik kuzatish bo'yicha mutaxassislar) bilan ta'minlash;



jamoatchilik o'rtasida imkoniyati cheklangan bolalarning bilim olish huquqi, inklyuziv o'qitishning mazmun-mohiyati haqida tushuntirish ishlarini olib borish;

ota-ona qaramog'isiz qolgan bolalarni tarbiyalashning muqobil shakllarini keng joriy etish;

o'quvchilarning jismoniy va aqliy talab-ehtiyojidan va ta'lim muassasalarining geografik joylashuvidan kelib chiqqan holda maxsus maktab-internatlarni optimallashtirish;

imkoniyati cheklangan bolalarning moslashishi va integratsiyasi uchun maktab-internatlarni bosqichma-bosqich maxsus jihozlar bilan ta'minlash;

imkoniyati cheklangan har bir bolaning inklyuziv ta'lim olishiga bo'lgan huquqini ta'minlashga qaratilgan chora-tadbirlarni belgilash.

Inklyuziv so'zi - fransuzcha **inclusif** "o'z ichiga olmoq" lotinchadan **includo** "o'z ichiga oladi" kabi ma'nolarni anglatadi.

**Inklyuziv ta'lim** tizimini rivojlantirishning **maqsadi** — ta'lim olish uchun teng imkoniyatni ta'minlash va barcha bolalarning individual xususiyatlaridan, oldingi ta'lim yutuqlaridan, tili, madaniyati, ota-onalarning ijtimoiy va iqtisodiy holatidan qat'iy nazar ta'limda muvaffaqiyatga erishishi uchun zarur shart-sharoitlarni yaratishdir.

**Inklyuziv ta'lim** vazifasi bolalarning qobiliyatlari va holatidan qat'i nazar, ularning barchasiga sifatli ta'lim taqdim etishdan iborat. Shu bilan birga, inklyuzivlik tamoyili imkoniyatlari cheklangan bolalar ijobiy ruhiy va ijtimoiy rivojlanishga ega bo'lishlari uchun oilada yashashlari va o'z tengdoshlari bilan birga oddiy maktabda bilim olishlari lozimligini nazarda tutadi. Inklyuziv ta'lim tizimi nogironlar aravachasidagi bola yaqin atrofda joylashgan har qanday maktabda ta'lim olishi, o'zlashtirishda qiynalayotgan bo'lsa, o'qish va yozishga o'rganish uchun maxsus yordamga ega bo'lishi, darslarga qatnamay qo'ygan bolaga esa maktabga qaytish uchun tegishli yordam ko'rsatilishini kafolatlaydi.

**Inklyuziv ta'limning sakkiz tamoyili:**

1. Insonning qadr-qimmati uning qobiliyati va yutuqlariga bog'liq emas;

2. Har bir inson his qilish va fikrlash qobiliyatiga ega;

3. Har bir inson muloqot qilish va uni eshitish huquqiga ega;

4. Hamma odamlar bir-biriga muhtoj;

5. Haqiqiy tarbiya faqat haqiqiy munosabatlar sharoitida amalga oshishi mumkin;

6. Hamma odamlar tengdoshlarining yordami va do'stligiga muhtoj;

7. Barcha o'quvchilar uchun taraqqiyot, ular qila olmaydigan narsadan ko'ra, qila oladigan narsada bo'ladi;

8. Xilma-xillik inson hayotining barcha jabhalarini oshiradi.

***O'zbekiston Respublikasida inklyuziv ta'lim tizimining joriy etilish masalalari***

O'zbekiston Respublikasida nogiron bolalar bilan bog'liq tahlil va dastlabki baholash ishlari 1966 yilda boshlangan.

Hozirgi kunda O'zbekistonda 250000 ga yaqin turli ko'rinishdagi nogiron bolalar (16 yoshgacha) ta'lim olish ehtiyojiga ega. Nogiron bolalar uchun ta'lim bilan birgalikda maxsus xizmatlar tashkil etish lozim. Ko'zi ojizlar, kar va eshitish nuqsoniga ega bo'lgan bolalar, poliyemiyelit bilan kasallanganlar, aqli zaif bolalar, nutqida nuqsoni bor va soqov bolalarga mo'ljallangan 86 ta maxsus ta'lim va aralashmaxsus muassasalar, 982 ta maxsus bolalar bog'chalari mavjud.

O'zbekistonda maxsus ta'lim sohasida quyidagi tadbirlar amalga oshirilmoqda:

- yordamga muhtoj bolalar uchun moslashuvchan va ko'p qirrali ta'lim tizimini yaratish;

- mahalliy va mintaqaviy miqyosda maxsus ta'limning tobora oshib borayotgan ahamiyati asosida ta'lim boshqaruvini markazlashtirish;

- yordamga muhtoj bolalarga yoshlikdan toshhis qo'yish va kasalpiklarni aniqlash uchun sharoit yaratish;

- milliy ta'lim standartlari asosida yordamga muhtoj bolalarga mo'ljallangon o'quv qo'llanmalar sifatini yaxshilash;

- ta'lim muassasalarining moddiy-texnika bozasini mustahkamlash;



- nogiron bolalar bilan ishlashga ixtisoslashgan xalqaro tashkilotlar bilan hamkorlik aloqalarini kengaytirish;

- ko'zi ojiz bolalar uchun mo'ljallangan turli kitoblar, metodologik adabiyotlarni chop ztish;

- nogiron bolalarni maxsus aravachalar, eshitish moslamalari, ko'zoynaklar, sport anjomlari, ish asbob-uskunalari, kanselyariya mollari, maxsus mebellar va tibbiy uskunalar bilan ta'minlash;

- maxsus talim sohasida kadrlar tayyorlash.

Hozirgi kunda qator ekologiq ijtimoiy va boshqa sabablarga ko'ra, shuningdek homiladorlikdan keyingi patologik asoratlar natijasida bola rivojlanishi va birinchi navbatda, uning ongi, atrof-muhit tahlili holda faoliyatini nazorat qilish va boshqarish funksiyalarining rivojlanish masalasini o'rganish muhimdir.

Ota-onalar qishloq sharoitida yordamga muhtoj bolalariga talab darajasida yordam ko'rsatish imkoniyatiga ega emas. Birinchidan, moddiy tomondan imkoniyat cheklanganligi, ikkinchi tomondan esa, yordamga muhtoj bolalarning go'dakligidan ularning nuqsonlarini aniqlash uchun o'qituvchi va psixologlarning malakasi talab darajasida emas.

Tarbiyachilar, psixologlar, o'qituvchilarning maxsus defektologiyaga asoslangan o'quv dasturlarda olgan bilim va malakalari ularning maxsus guruhlardagi faoliyatlari davomida aniq tashhis qo'yish va sifatli davalashni amalga oshirish imkoniyatini yaratadi.

*Inklyuziv ta'limning asosiy maqsadi* — yordamga muhtoj bo'lgan bolalarga samarali bilim olish uchun sharoit yaratishdir.

Ushbu sharoitda yordamga muhtoj bolalarni integrasiyalash va reabilitasiya qilish, har bir bolaning rivojlanish darajasini hisobga olgan holda ularga mos samarali inklyuziv talim turini tanlash lozim.

1996 yilning noyabr oyida YuNESKO ishlari bo'yicha O'zbekiston Milliy komissiyasi tashabbusi asosida Toshkentda «Maxsus ta'lim sohasida inklyuziv usullar» movzusida milliy o'quv dastur muvaffaqiyatli amalga oshirilgan. 1998

yilning oktyabr oyida Buxoro shahrida ushbu mavzu bo'yicha mintaqaviy anjuman tashkil etilgan edi. Mazkur anjuman YuNESKO, YuNISEF (BMTning bolalar jamg'armasi), Butunjahon sog'liqni saqlash tashkiloti va Xalqaro mehnat tashkiloti bilan hamkorlikda amalga oshirilgan. Ushbu tadbirlar notijosida 2001 yilda O'zbekiston Xolq ta'limi vazirligi qoshida Inklyuziv ta'lim bo'yicha manba markazi tashkil etildi. Hozirgi kunga qadar ushbu markaz tomonidan bir necha o'quv seminarlari o'tkazildi va qator dasturlar amalga oshirib kelinmoqda.

2004 yilning iyun oyida «Sen yolg'iz emassan» respublika jamoatchilik bolalar jamg'armasi tashabbusi asosida Toshkent shahrida «Yetim bolalarning ijtimoiy muhofozasi» mavzusida ilk bor xalqaro anjuman tashkil etildi. Ushbu anjuman doirasida nogiron bolalar uchun talim dasturlari ham muhokama etildi.

2005 yilning may oyida Toshkent shahrida Respublika bolalar mjtimoiy moslashuvi markazi va «Sen yolg'iz emassan» respublika jomoatchilik bolalar jamg'armasi tomonidan «Ijtimoiy nochor bo'lgan bolalarga ko'mak berishning samarali shakl va usullari» nomli xalqaro forum o'tkazilgan edi. Ushbu forum tavsiyanomalari asosida YuNESKO ishlari bo'yicha O'zbekiston Respublikasi Milliy komissiyasi O'zbekiston Xalq ta'limi vazirligi bilan hamkorlikda YuNESKO tashkiloti rahnamoligida Osiyo va Tinch okeani mintaqasidagi madaniy markaziga (Tokio, Yaponiya) maxsus loyiqa taqdim etilgan edi. Ushbu YuNESKO markazi tomonidan «O'zbekistonda inklyuziv ta'limni joriy etish bo'yicha bog'cha va o'rta maktablarda tajribaviy guruhlar ochish» nomli loyiha qo'llab-quvvatlandi va yaqin kunlarda amalga oshirilishi rejalashtirilmoqda.

Loyihaning asosiy maqsadi nogiron bolalarda turfa xil malakalarni oshirish va ularning qobiliyatlorini barqaror rivojlantirish uchun sharoit yaratishdan iborat.

Ta'lim tibbiy va ijtimoiy xizmat bilan birgalikda olib boriladi. Oila va maqallada ota-onalar uchun profilaktika hamda reabilitasiya ishlari bo'yicha o'quv mashg'ulotlari tashkil etiladi. Ota-onalar nogiron bolalarini tarbiyalash va ularning aqliy rivojlanishlarini rag'batlantirish bo'yicha pedagogik usullar, shuningdek ularning mustaqil bo'lishlari uchun tengdosh sog'lom bolalar bilan muloqot qilishlari bo'yicha o'qitiladilar.



Loyiha to'qqiz bosqichdan iborat bo'lib, har bir bosqich quyidagi faoliyatlarni qamrab oladi:

1-bosqich: Respublika ta'lim markazi qoshidagi Maxsus talim bo'yicha manba markazida ko'chma ta'lim guruhi tashkil etiladi. Ko'chma ta'lim guruhiga texnik yordam ko'rsatish.

2-bosqich: «Barqaror toraqqiyot uchun inklyuziv ta'lim» mavzusida milliy anjuman tashkil etish.

3-bosqich: Xalq ta'limi vazirligining viloyat boshqormalori bilan hamkorlikda nuqson bilan rivojlanoyotgan bolalarni aniqlash bo'yicha tibbiy-psixologik-pedogogik komissiyani tashkil etish. Qo'shma guruh va sinflarda o'qitish moqsadida nuqson dorajosi me'yordon og'ishgon (3-7 yoshdagi) bolalarni aniqlash.

4-bosqich: Uslubiy tavsiyanomalar, qo'llanmalar va dasturlarni nashr qilish.

5-bosqich: Pedagog-tarbiyachilar, o'qituvchilar, psixologlarning qo'shma guruhlari va sinflarda bolalardagi nuqsonlarni tuzatish va rivojlantirishga yo'naltirilgan dasturlarini ishlab chiqish bo'yicha o'quv mashg'ulotlarini tashkil etish.

6-bosqich: Mavjud bolalar ta'limi muassasalarida, 2 ta bog'cha va 2 ta o'rta maktabda maxsus tajribaviy guruh tashkil etish, Texnik yordam ko'rsatish.

7-bosqich: Maktabgacha inklyuziv ta'lim Ixtisoslashgan ishlab chiqilgan tajribalarni targ'ib qilish bo'yicha ilmiy-uslubiy, amaliy-mintaqaviy anjumanni tashkil etish.

8-bosqich: Monitoring va baholash.

9-bosqich: Moliyaviy hisobot.

Loyiha yordamga muhtoj bolalar, ularning ota-onalari, bog'cha pedagog-tarbiyachilariga qaratilgan.

Loyiha Respublika ta'lim markazi qoshidagi Inklyuziv ta'lim bo'yicha manba markazi tomonidan Toshkent Davlat pedagogika universitetining Boshlang'ich ta'lim va defektologiya fakulteti, YuNESKOning O'zbekistondagi

vakolatxonasi va YuNESKO ishlari bo'yicha O'zbekiston Milliy komissiyasi, shuningdek boshqa mutasaddi tashkilotlar bilan hamkorlikda amalga oshiriladi.

Inklyuziv ta'lim bo'yicha manba markazi 2001 yilda O'zbekiston Xalq talimi vazirligi huzuridagi Respublika ta'lim markazida tashkil etilgan.

Tashkilotning asosiy faoliyati quyidagilardan iborat:

- nogiron bolalar ta'limi sohasida faoliyat ko'rsatuvchi o'qituvchi va tarbiyachilar uchun turli anjuman va o'quv mashg'ulotlarini tashkil etish orqali O'zbekiston Respublikasi ta'lim tizimiga inklyuziv ta'limni tatbiq etish;
- nogiron bolalar uchun o'quv darsliklarini yaratish;
- nogiron bolalar uchun tajribaviy maydonlar barpo etish;
- bola uchun alohida rivojlantirish rejasini yaratish;
- pedagoglar va ota–onalarga maslahat xizmatini ko'rsatish;
- uslubiy qo'llanmalar, tavsiyanomalar, maxsus maktablarda nogiron bolalar bilan ishlash rejasini yaratish;
- yuridik faoliyat va ijtimoiy muhofaza bo'yicha ma'lumot bilan ta'minlash;
- nogiron bolalar ta'limi sohasida faoliyat yurituvchi jamoat va davlat tashkilotlari bilan hamkorlik qilish;
- nogiron bolalar ta'limi sohasida mavjud kamchiliklarni ommaviy axborot vasitalarida yoritib borish;
- xalqaro tashkilotlar bilan hamkorlik qilish; maxsus ta'lim sohasidagi tajribalarni tatbiq etish.

Ta'lim sohasida yordamga muhtoj bolalarning tahsil olishlari hamisha jamiyatning diqqat markazida turgan dolzarb masala hisoblanadi. Shunday ekan, ularga ta'lim beruvchi pedagoglar va mutaxassislor malakasini oshirish, zarur zamonaviy qo'llanmalar, jihozlar bilan ta'minlash ham bu masalani hal qilish uchun qo'yilgan qadamlardan biri hisoblanadi.

BMT tomonidan 1989 yilda qabul qilingan «Bola huquqlari to'g'risidagi»gi Konvensiyasi hamma bolalarni, shu qatori maxsus ehtiyojli bolalar



huquqlarini ham himoya qiladi va qo'llab-quvvatlaydi. Aynan 2, 23, 28, 29 - moddalarda maxsus ehtiyojli bolalari huquqlari belgilangan.

Bolalar huquqlari To'g'risidagi Konvensiyaning 2-moddasi maxsus yordamga muhtoj bolalar uchun asosiy modda hisoblanadi. Unda mazkur Konvensiyadagi har bir modda irqi, dini, millati, etnik yoki ijtimoiy kelib chiqishidan qat'iy nazar barcha bolalaga tegishliligi haqida ta'kidlanib, "Barcha huquqlar har bir bola uchun tegishli. Kamsitish yoki jazolashning barcha shakllaridan bolaning himoyasini ta'minlash uchun zarur choralarni ko'rish ishtirokchi davlatlar majburiyatlariga kiradi" deb bayon qilingan.

Shuningdeq Bolalar huquqlari to'g'risidagi Konvensiyaning 23-bandida maxsus ehtiyojli bolalarning ta'limi xususida quyidagicha ta'kidlangan "Nogiron bolani maxsus ehtiyojlarini aniqlab, uni ijtimoiy hayotga qo'shishi va shaxs sifatida rivojlana olishiga yetaklovchi vasita hisoblanadigan ta'lim olishga har tomonlama yordam berishi lozim. Ishtirokchi davlatlar aqliy va jismoniy jihatdan yaxshi rivojlanmagan bola o'zining qadr-qimmatini ta'minlaydigan, o'ziga ishonch tug'diradigan va uning jamiyat hayotidagi faol ishtirokini yengillashtiradigan sharoitlarda yashashlarini ta'minlaydilar".

Maxsus ehtiyojli bolalrni umumta'lim muassasalari tizimida o'qitish ularning haq-huqularni ta'minlaydi. Shuning uchun Bolalar huquqlari to'g'risidagi Konvensiya maxsus ehtiyojli bolalarni huquqlarni ta'minlaydigan asosiy huquqiy me'yoriy hujjatdir.

Nogironlarni umumta'lim tizimida o'qitish masalalariga e'tibor berish Respublikamizda 1996 yilda O'zbekiston Respublikasi Xalq Ta'limi Vazirligi, Respublika ta'lim markazi va YuNESKO tashkiloti bilan hamkorlikda respublika seminari o'tkazilishi bilan islohotlar amalga oshirila boshladi. Shu davrdan boshlab olimlar, maxsus ta'lim tizimidagi rahbar xodimlari, pedagoglar, umumta'lim mussasalarining rahbarlari va nodavlat jamoa tashkilotlarining nogironlar ta'limi ehtiyojini qondirishga qaratilgan munosabatlari o'zgara boshladi.

Respublika Ta'lim Markazining maxsus ta'lim bo'limi hodimlari imkoniyati cheklangan bolalarni integrasiyalashgan ta'lim jarayonida ta'lim olish strategiyasini keng joriy qilish maqsadida YuNESKO tashkiloti bilan 1996 yildan buyon hamkorlik qilib kelmoqda. O'zbekistonda integrasiyalashgan inklyuziv ta'lim tizimini amaliyotga tadbiq qilish maqsadida YuNESKO xalqaro tashkiloti loyihasi asosida bir necha Respublika seminar-treninglari va xalqaro konferensiyalar o'tkazishga muyassar bo'lindi. Konferensiyalarda ko'tarilgan dolzarb muammolar, masalalar, tavsiyalar va ishtirokchilarning ma'ruzalari xalqaro toplamda chop etildi va ommaga tarqatildi. Hozirgi kunda Respublikamizda inklyuziv ta'lim konsepsiyasini joriy qilishda asosiy dasturamal bo'lib kelmoqda.

1998 yilda YuNESKO tashabbusi bilan Buxoro shahrida yirik Konferensiya o'tkazildi. Konferensiyaning maqsadi alohida yordamga muhtoj bolalarni ijtimoiy qo'llash, reabilitasiya qilish, ta'limga jalb qilish, moddiy, texnikaviy yordamlarni tashkil qilish va ularni to'laqonli jamiyatga moslashtirishga oid turli tashkiliy uslubiy ishlarni amalga oshirishda Markaziy Osiyoda ko'p tarmoqli aloqalar o'rnatish edi.

***Imkoniyati cheklangan insonlar uchun yaratilgan dasturlar***

Ko'pgina nogironlar uchun zarur bo'lgan texnik jihozlardan tashqari, ish stoli kompyuter yoki noutbukda to'liq yoki hech bo'lmaganda qisman ishlash uchun jismoniy imkoniyati cheklangan odamlar uchun moslashtirilgan maxsus dasturiy ta'minot ham talab qilinadi. Bunday dasturlarni kompyuter texnologiyalari imkoniyatlari bilan ifodalanadigan ko'pchilik qo'llash sohalarini qamrab oluvchi bir qancha toifalarga bo'lish mumkin:

lupalar yoki ekranni kattalashtirish tizimlari;

o'qish dasturlari;

Skanerlash va matnni aniqlash uchun dasturiy ta'minot;

dasturiy manipulyatorlar va kiritish qurilmalari;

navigatsiya dasturlari;



aloqa vositalari.

Ko'pgina hollarda, kompyuter bilan ishlashda sezilarli muammolar ko'rish muammolari bilan og'rigan foydalanuvchilar tomonidan uchraydi. Aynan shu fuqarolar uchun bir qator rivojlanish kompaniyalari maxsus ilovalar va dasturlarni yaratdilar va yangilashda davom etmoqdalar, ammo ularning narxi ko'p hollarda mahalliy iste'molchilar uchun chidab bo'lmas bo'lib qolmoqda. Bozordagi bepul yoki arzon analoglar juda eskirgan va zamonaviy operatsion tizimlarda ishlashga moslashtirilmagan, nogiron foydalanuvchilar uchun imkoniyatlar doirasini sezilarli darajada toraytiradi.

Ko'zi ojiz yoki zaif ko'ruvchi foydalanuvchi uchun avtomatlashtirilgan ish joyining dasturiy-apparat kompleksi:

Nutq sintezi bilan ekranni o'qish dasturi;

Nutqni qo'llab-quvvatlaydigan ekran kattalashtirish dasturi;

Brayl klaviaturasi;

Brayl display;

Akustik tizim;

hujjat kamerasi;

elektron lupa;

Masofadan ko'rish uchun video kattalashtiruvchi.

Eshitish qobiliyati buzilgan foydalanuvchilar uchun avtomatlashtirilgan ish joyining apparat-dasturiy kompleksi:

Akustik tizim;

radio sinfi;

Portativ induksion tizimi;

Tayanch-harakat tizimi buzilgan foydalanuvchilar uchun avtomatlashtirilgan ish joyining dasturiy-apparat kompleksi:

Katta dasturlashtiriladigan Clavinta klaviaturasi;

Moslashtirilgan sichqoncha;

Rolikli kompyuter;

Simsiz qabul qiluvchi (bir nechta simsiz qurilmalarni ulash uchun);

*Imkoniyati cheklangan bolalarga ko'rsatiladigan ta'lim xizmatlari*

Imkoniyati cheklangan bolalarni masofaviy ta'lim jarayonini ta'minlash maqsadida masofaviy ta'limning quyidagi vositalari qo'llaniladi: multimediali ixtisoslashtirilgan darsliklar, elektron o'quv-uslubiy majmualar, shu jumladan elektron darsliklar, o'quv qo'llanmalari, o'quv kompyuter dasturlari, kompyuter laboratoriyalari ustaxonalari, nazorat va sinov to'plamlari, o'quv videolari, audio yozuvlar, telekommunikatsiya va boshqa aloqa kanallari orqali kompyuter texnikasi, raqamli o'quv uskunalari, orgtexnika va nogiron bolalarning rivojlanish nuqsonlari xususiyatlariga moslashtirilgan dasturiy ta'minot orqali uzatish uchun mo'ljallangan boshqa materiallar.

Bugungi kunda jahonning yetakchi universitetlarining texnologik taraqqiyoti shunday chegaraga yetdiki, axborot bazasini yanada rivojlantirish sifat jihatidan yangi o'zgarishlarni keltirib chiqarmaydi. Elektron ta'lim endi yangilik emas, unda noaniq pozitsiyalar yo'q. Talabalar uchun jamoat mulki bo'lgan ta'lim mazmuni, o'qituvchilar va talabalarga fikr-mulohazalarni taqdim etish, ular o'rtasida bilim almashish, ma'muriy vazifalarni avtomatlashtirish - bularning barchasi texnologiyaga tegishli. Shu sababli, elektron ta'limning asosiy vazifasi - o'quvchilarning psixofizik xususiyatlari va cheklovlarini hisobga olgan holda o'qitishni individuallashtirish.

Nogironlarga nisbatan zamonaviy mahalliy va xorijiy ta'lim metodologiyasi ular uchun asosiy cheklovlar aloqa va ma'lumotlarga kirish ekanligini ta'kidlaydi. Shubhasiz, turli jismoniy nuqsonlari bo'lgan nogiron talabalar uchun masofaviy ta'lim o'ziga xos xususiyatlarga ega bo'lishi kerak. Nogironlar va nogironlarni o'qitishda elektron ta'lim va masofaviy ta'lim texnologiyalari ular uchun mavjud bo'lgan shakllarda ma'lumotlarni olish va uzatish imkoniyatini ta'minlashi kerak.

Nogironlar va imkoniyati cheklangan bolalar uchun elektron ta'limni joriy qilishda ta'limning qulayligi va sifatiga ta'sir qiluvchi uchta komponent mavjud:

- elektron ta'limni tashkil etish vositalari (kontentni boshqarish tizimlari, ta'limni boshqarish tizimlari va boshqalar);
- ta'lim mazmuni;



- pedagogik o'zaro ta'sir (shakllar, usullar, pedagogik texnologiyalar va boshqalar).

Ta'lim saytlarini ishlab chiqishda eng boshidanoq interfeys ham, kontent ham eng ko'p o'quvchilarning ehtiyojlarini qondirishga, ya'ni universal dizaynga ega bo'lishini ta'minlashga e'tibor qaratish lozim. Universal dizayn - bu barcha odamlarga moslashtirilgan yoki shaxsiy dizaynga ehtiyoj sezmasdan maksimal darajada foydalanishi mumkin bo'lgan mahsulotlar, muhitlar, dasturlar yoki xizmatlarning dizayni.

**Nazorat savollari**

1. O'zbekiston Respublikasida nogiron bolalar bilan bog'liq tahlil va dastlabki baholash ishlari nechinchi yilda boshlangan?
2. O'zbekistonda maxsus ta'lim sohasida qanday tadbirlar amalga oshirilmoqda?
3. Inklyuziv ta'limning asosiy maqsadi nima?
4. 2004 yilning iyun oyida qanday xalqaro anjumanlar tashkil etildi?
5. YUNESKO markazi tomonidan «O'zbekistonda inklyuziv ta'limni joriy etish bo'yicha bog'cha va o'rta maktablarda tajribaviy guruhlar ochish» nomli loyiha nechta bosqichdan iborat?
6. BMT tomonidan nechanchi yilda «Bola huquqlari to'g'risidagi»gi Konvensiyasi qabul qilingan?
7. Ko'zi ojiz yoki zaif ko'ruvchi foydalanuvchi uchun avtomatlashtirilgan ish joyining dasturiy-apparat komplekslari nima?
8. Eshitish qobiliyati buzilgan foydalanuvchilar uchun avtomatlashtirilgan ish joyining apparat-dasturiy komplekslari nima?
9. Tayanch-harakat tizimi buzilgan foydalanuvchilar uchun avtomatlashtirilgan ish joyining dasturiy-apparat komplekslari nima?

## III BOB. ELEKTRON PEDAGOGIKADA PORTFOLIO VA O'QITISH TIZIMLARINI TASHKIL ETISH SHAKLLARI

### *3.1.* Elektron portfolio bilan ishlash va uni shakllantirish

*Pedagogning portfoliosi haqida tushuncha*

Ta'lim-tarbiya jarayonlarini modernizasiyalashtirish ijodiy fikrlovchi, ta'limning zamonaviy metod va texnologiyalarini, pedagogik-psixologik diagnostika usullarini, aniq amaliy faoliyat asosida pedagogik jarayonni mustaqil loyihalash usullarini qo'llay oladigan pedagoglar tarkibini shakllantirishni talab etadi.

Hozirgi kunda pedagoglarga nisbatan o'zining samarali faoliyatini tashkil qilishda o'quv, ilmiy hamda madaniy-ma'rifiy tadbirlarni to'g'ri rejalashtirishi va amalga oshirishi, kasbiy pedagogik mahoratini uzluksiz oshirib borishda o'zgarib boruvchi zamonaviy talablarga tezkor ravishda moslashib borish kabi talablar qo'yilmoqda. Chunonchi, pyedagog kadrlarning ta'lim-tarbiya jarayonlaridagi raqobatbardoshligi uning ilg'or ta'lim texnologiyalarini o'zlashtirish qobiliyati, o'zgaruvchan hamda oshib borayotgan kasbiy talablarga moslasha olishiga bog'liq.

Bugungi kunda zamonaviy axborot-kommunikasiya texnologiyalarini pedagogik faoliyat hamda kasbiy kompetentlikning ajralmas qismi sifatida shakllantirish ustuvor yo'nalish sifatida qaralmoqda. Shu sababdan pedagoglarning kasbiy ma'lumotlar bazasi va talabalar bilan o'quv muloqotlarini elektron resurslar asosida tashkil etish pedagogik jihatdan muhim vazifalar qatoriga kiradi. Bunday vazifalar pedagog kadrlarning elektron portfoliosini ishlab chiqishni taqozo etadi.

"Portfolio" tushunchasi XV-XVI asrlarda G'arbiy Yevropadan kirib kelgan bo'lib, uyg'onish davrida arxitektorlar o'z buyurtmachilariga qurilish loyihalarini tayyor va homaki variantlarini "portfolio" deb nomlangan alohida papkada taqdim etishgan. Ushbu papkada taqdim etilgan hujjatlar talabgorda qurilish loyihasining kasbiy sifatlari haqida taassurot hosil qilgan.

Hozirgi vaqtda esa biznes olamida portfolio firmaning yutuqlarini ko'rsatish, fotosuratchi va fotomodellar sohasida esa – suratlar albomi sifatida ishlatiladi.



Portfolioni ta'lim sohasida qo'llash g'oyasi, 80-yillarning o'rtalarida AQSHda paydo bo'ldi. AQSH va Kanadadan so'ng, portfolio g'oyasi Yevropa va Yaponiyada ommalashdi, XXI asrning boshlarida esa bu g'oya Rossiyada keng tarqaldi va hozirgi kunda bu g'oya O'zbekistonda ham keng yoyilmoqda.

Portfolio (ingl. – portfel, zarur ishlar va hujjatlar uchun papka. frans. – bayon qilmoq, ifoda etmoq, tashimoq. ital. – hujjatlar solingan papka) – bu hujjatlar, ish namunalari, fotosuratlar, taqdim etilayotgan imkoniyatlarni tasavvur eta olish imkoniyatini beruvchi materiallar, mutaxassis xizmatlari to'plamidan iborat.

Pedagogning portfoliosi quyidagi imkoniyatlarga ega:

- pedagogning ma'lum bir vaqt oralig'ida erishgan kasbiy yutuqlari va faoliyat natijalarini qayd etish usuli;
- faoliyati davomida kasbiy sohadagi erishilgan yutuqlarini namoyish etuvchi majmua;
- pedagogning dars berayotgan fani bo'yicha o'quv materiallarini talabalarga yetkazib beruvchi vosita;
- pedagog va talabalar o'rtasidagi o'quv muloqotini ta'minlashga xizmat qiluvchi tizim;
- talabalar bilan teskari aloqani o'rnatishga xizmat qiluvchi hamda bilimlarni o'zlashtirish jarayonini monitoring qilish tizimi.

Pedagogning portfoliosi ta'lim muassasalari rahbariyati uchun o'qituvchilarning ish faoliyati unumdorligini monitoringini olib borish va yana ham muhim tomoni o'qituvchilarni o'z-o'zini kuzatish va o'z ustida ishlashi uchun muhim vosita hisoblanadi. Turli manbalardagi ma'lumotlarga ko'ra pedagog portfoliosi – bu o'qituvchining aniq faktlar asosida yozilgan pedagogik sifati va yutuqlari hisoblanadi. Bundan tashqari portfolioda o'qituvchining individual yutuqlari, turli loyihalarda qatnashganliklari, talabalarining fan olimpiadalari, tanlovlar, musobaqalarda g'olib bo'lganliklari qayd etib boriladi. Shu bilan birga pedagog portfoliosi pedagogik-psixologik diagnostika natijalari, talabalar uchun fanlar bo'yicha nazorat qilish topshiriq va testlarini qamrab oladi.

Portfolio joriy etilishi bilan pedagogik faoliyatni baholashning va o'zo'ziga baho berishning ko'p funksiyali vositasi shakllanadi. Bunda portfolio qator pedagogik masalalarni yechishda yordam beradi:

- ta'lim berishda yuqori motivasiyani rivojlantirish;
- talabalarning mustaqil ta'limi va o'z ustida ishlashga intilishni oshirish;
- uzluksiz rivojlanishni rag'batlantiruvchi omilni joriy etish;
- bilimlarning samarali o'zlashtirilishiga intilish;
- pedagogik faoliyat natijalarini tashhis qilish.

Bundan tashqari portfolio o'qituvchiga o'z yutuqlarini yanada kengroq va xilmaxil taqdim etish imkonini beradi.

***Elektron portfolio tizimi va uni tashkil etish turlari***

**Elektron portfolio** — boshqaruv va pedagog kadrlarning kasbiy faoliyati natijalarini baholashda ko'maklashishga qaratilgan o'quv-metodik, ilmiy-tadqiqot va ijodiy ish materiallarini qamrab oluvchi elektron resurslar majmuasi.

Portfolio quyidagi ko'rinishlarda bo'lishi mumkin:

- portfolio sayti (sayt ko'rinishidagi portfolio);
- veb sahifa (biror sayt tarkibidagi shaxsiy sahifa);
- elektron taqdimot;
- natijalar papkasi.

Elektron portfolio ko'rgazmaliligi, qulayligi, resurslarining aniq tuzilishiga egaligi bilan bir qatorda yana bir qancha o'ziga xos xususiyatlar va afzalliklarga ega:

- zamonaviyligi;
- tezkorligi (kerakli o'zgarishni tezda kiritish imkoniyati);
- funksionalligi (katta sondagi ekspertlarga, hamkasb- mutaxassislarga, qiziquvchilarga o'z tajribasini namoyish etish ikmoniyati) hamda o'z muvaffaqiyatlarini qayd etib borish, bir vaqtning o'zida doimiy ravishda to'ldirib borish mumkin bo'lgan raqamli ta'lim resurslarining tizimlashtirilgan mediatekasini yaratish imkoniyatining mavjudligi;



- effektivligi (o'qituvchini o'z-o'zini baholashi, boshqaruvchi hamda talabalarga ijobiy ta'sir ko'rsatish);

Portfolioning taqdimot shakli ma'lumotlarni ko'rgazmali tarzda namoyish etishni amalga oshirsa, sayt-portfolio shakli esa ko'proq ma'lumot olish va izlash imkoniyatini beradi. Internet izimining o'quv jarayoniga keng joriy etish bo'yicha yaratilgan imkoniyatlar portfolioning sayt-portfolio shaklida yaratish va uning resurslarini doimiy yangilanib borishini markazlashgan holda tizimli yo'lga qo'yish orqali samara berishi mumkin. Shuning uchun portfolioni tarmoqda saytportfolio sifatida joylashtirilishi maqsadga muvofiq.

Portfolioning muhim jihati – pedagogning kasbiy kompetentligini baholash uchun amaliy faoliyatdagi natijalarini (bajargan loyihalari, talabalarining olimpiada va tanlovlarda qatnashganligi, olib borgan ilmiy izlanishlari kabilarni) namoyish etishdan iborat. Portfolio o'qituvchiga o'z ishlari natijalarini tahlil etish, umumlashtirish, tizimlashtirish, o'z imkoniyatlarini ob'ektiv baholash va qiyinchiliklarni bartaraf etishni rejalashtirish hamda yuqori natijalarga erishish imkoniyatini beradi.

Portfolio resurslarini shakllantirishda quyidagi jihatlarga ahamiyat berish maqsadga muvofiq:

- tizimlilik;
- taqdimotlilik;
- yutuqlarni haqqoniy, to'g'ri baholash;
- taqdim etilayotgan axborotlarning to'liqligi, aniqligi va ishonchliligi;
- ma'lumotlarning ob'yektivligi.

Shunday qilib, portfolio pedagogik faoliyatning turli xil ko'rinishlarida (o'quv, tarbiyaviy, ijodiy, metodik, tadqiqot) o'qituvchi tomonidan erishilgan yutuqlarini yuzaga chiqarish imkonini beradi.

Bir qancha mualliflar o'z maqolalarida elektron portfolioni bir nechta variantlarini taklif etishgan:

• yutuqlar portfoliosi – ushbu portfolioda ahamiyat faoliyatdagi yutuqlarni tasdiqlovchi hujjatlarga qaratiladi;

• taqdimot portfoliosi – o'qituvchining eng yaxshi ishlari to'plami, ushbu portfolio yangi ishga kirayotganda, suhbatdan o'tish uchun yoki turli tanlovlarda qatnashish uchun kerak bo'ladi;

• hisobot ko'rinishidagi portfolio – biror-bir loyiha ishini tugatayotgan vaqtda bajarilgan ishlar va erishilgan yutuqlar haqida ma'lumot beradi;

• majmuaviy portfolio – yuqorida ko'rsatilgan portfolio ko'rinishlarini qamrab oladi va o'qituvchi portfoliosini namoyish etishga xizmat qiladi.

Oliy ta'lim muassasalari o'qituvchisining elektron portfoliosi quyidagi asosiy turlarga yo'naltirilishi zarur:

1. O'qituvchi haqida ma'lumotlar: portfolioning ushbu bo'limida: familiya, ismi, otasining ismi, tug'ilgan yili; ma'lumoti (ta'lim muassasasi nomi, bitirgan yili, mutaxassisligi va diplom bo'yicha ixtisosligi); mehnat va pedagogik tajribasi, ushbu ta'lim muassassidagi ish tajribasi; malaka oshirish (kurslarda tinglangan tizim nomi, yili, oyi, kurslar problematikasi); kasbiy rivojlanish individual rejasi, unda belgilangan maqsadlar va o'z kasbiy o'sishi vazifalari, egallashi kerak bo'lgan malakalar, yaqin 2–3 yil mobaynida o'tishni maqsad qilib qo'ygan treninglari va kurslari (o'qituvchining kasbiy rivojlanish maqsadlari va vazifalari o'qitiladigan fani kasbiy standartlari, talabalarning o'zlashtirishlari, oliy ta'lim muassasasi rejasiga mos bo'lishi kerak); ilmiy va faxriy unvon va darajalari mavjudligini tasdiqlovchi hujjatlar nusxalari; hukumat mukofotlari, yorliqlari, minnatdorchilik nomalari; turli tanlovlar diplomlari; attestatsiyadan o'tuvchining ixtiyori bo'yicha boshqa hujjatlar.

2. «Pedagogik faoliyat natijalari» (sxemalar, grafiklar va jadvallar ko'rinishida 3 yil davomidagi o'quv fani sohasidagi yutuqlari dinamikasi, jumladan, kirish imtihonlari) — portfolioning ushbu bo'limida talabalarning ta'lim dasturlarini o'zlashtirishlari natijalarini va pedagog o'qitadigan fanlar bo'yicha ularda shakllangan asosiy malakalarni ifoda etuvchi materiallar, quyidagilar asosida 3 yil davomidagi:



• bilimlari nazorat o'lchamlari;

• talabalarning oraliq va yakuniy attestatsiyalari natijalari;

• iqtidorli talabalar mavjudligi;

• bitiruvchilarning magistraturaga o'qishga kirishlari;

• talabalarning fan yo'nalishi bo'yicha magistraturaga kirishlari haqidagi ma'lumotlar;

• talabalarning tuman, shahar, mintaqaviy va respublika olimpiadalari, tanlovlarida ishtirok etishlari kabi pedagog faoliyati tahlili joylashtiriladi.

3. «Ilmiy-metodik faoliyat» (o'quv va tarbiyaviy ishlarda zamonaviy ta'lim texnologiyalaridan foydalanish): pedagog tomonidan tanlagan ta'lim dasturlari va o'quv-metodik adabiyotlar to'plamini asoslab beruvchi materiallar; pedagog tomonidan foydalaniladigan ta'lim texnologiyalarini asoslab beruvchi materiallar; pedagog tomonidan o'z amaliy faoliyatida qo'llaydigan ta'lim natijalarini baholash uchun u yoki bu pedagogik diagnostika vositalari berilgan materiallar; ta'lim jarayonida axborot-kommunikatsiya texnologiyalaridan foydalanilishi bo'yicha materiallar, rivojlanish muammolari bilan talabalarni o'qitish metodik texnologiyalari; metodik birlashmalarda ishlashi, oliy ta'lim muassasasi metodik markazi, boshqa OTMlar va boshqa muassasalar bilan hamkorligi to'g'risidagi materiallar; hisobot materiallari, kasbiy va ijodiy pedagogik tanlovlarda ishtirok etishi, seminarlar, «davra suhbatlari», master-klasslar va shu kabilarni tashkil etish va o'tkazish; ilmiy tadqiqotlar o'tkazish; mualliflik dasturlarini ishlab chiqish; doktorlik dissertatsiyasi qo'lyozmasini yozish; ijodiy hisobot, referat, hisobotlar, maqolalar tayyorlashdan iborat.

4. «Fan bo'yicha darsdan tashqari faoliyat»: Talabalarning fan bo'yicha bajargan ijodiy ishlari, referatlari, o'quv-tadqiqotchilik ishlari, loyihalari ro'yxati; olimpiadalar, tanlovlar, musobaqalar, intellektual marafonlar va boshqalar g'oliblari ro'yxatlari; sinfdan tashqari tadbirlar ssenariylari, o'tkazilgan tadbirlar fotosuratlari va videomateriallari (ko'rgazmalar, fan ekskursiyalari, tanlovlar, breyn-ringi va boshqalar); to'garaklar va fakultativlar dasturlari; boshqa materiallardan iborat.

5. «O'quv-moddiy bazasi» (pedagogning o'z kabinetini metodik jihozlashga qo'shgan hissasi):

• fan bo'yicha lug'atlar va boshqa axborot adabiyotlarning mavjudligi;

• ko'rgazmali qo'llanmalarning mavjudligi (maketlar, jadvallar, sxemalar, illyustratsiyalar, portretlar va boshqa-lar);

• didaktik materiallar, masalalar, mashqlar to'plamlari, referatlar va insholar namunalari va shu kabilarning mavjudligi;

• talabalar bilimlari sifati o'lchamlari;

• texnik vositalarning mavjudligi (televizor, videomagnitofon, musiqa markazi, diaproyektor, kompyuter va ta'lim kompyuterli vositalari, audio va video qo'llanmalar);

• doimiy foydalaniladigan o'quv texnik vositalari haqidagi ma'lumotlar;

• didaktik materiallar, masalalar, mashqlar to'plamlari, referatlar va insholar namunalari va shu kabilardan, magistraturaga kirish imtihonlariga tayyorlanishi bo'yicha materiallardan foydalanish;

• pedagog ixtiyori bo'yicha boshqa hujjatlar.

6. «Guruh rahbari sifatida pedagogning vazifalari»: guruh talabalari o'zlashtirishlari va bilimlari sifati tahlili; guruhda talabalar tartibi saqlanib qolishi haqida ma'lumotlar; huquqbuzarliklar haqidagi ma'lumotlar; ota-onalar bilan ishlash haqidagi ma'lumotlar; guruh rahbari soatlari va ota-onalar majlislari ishlab chiqilishidan iborat.

7. «O'z pedagogik faoliyati natijalarini baholash».

8. «Taklif va mulohazalar» — talabalar, hamkasblari, ma'muriyat, ota-onalar baholari.

Portfolioni tayyorlash

Pedagog portfoliosi pedagogning o'zi tomonidan papkada — fayllar to'plamida qog'ozda hamda elektron ko'rinishda tayyorlanadi. Portfolioga kiritilgan har bir alohida material (yorliqlar, tashakkurnomalardan tashqari) sanasi qo'yilishi va imzolanishi kerak.



Portfolioni baholash. Portfolio ta'lim muassasasi ma'muriyati yoki taqdim etilishi maqsadiga qarab jamoat organi tomonidan baholanadi. Baholashda portfolio barcha materiallari talabalar natijalariga, pedagog malakasini oshirishga qanday ta'sir ko'rsatganligi nuqtai nazaridan ko'rib chiqiladi. Shu tariqa, pedagog elektron portfeli bir tomondan, pedagogning shaxsiy portfoliosi, ikkinchi tomondan, boshqa pedagoglar, metodistlar, IT-mutaxassislar tajribalarini birlashtirish va anglab yetish hisoblanadi. Unda pedagog hamda uning talabalari mustaqil va ijodiy faoliyatlari uchun o'rin ajratiladi. Bundan tashqari, kompyuter hamda Internet tarmog'i yordamida ta'lim muhitida boshqa pedagoglar, talabalar bilan muloqotlar va o'zaro aloqalarda (elektron seminarlar, maslahatlar, veb-loyihalar va shu kabilar) namoyon bo'ladigan elektron portfolioni ishlab chiqishda hamda foydalanishdagi kommunikativ rolini alohida ta'kidlab o'tamiz.

Elektron portfelni yaratish uchun: Microsoft FrontPage, Adobe Dreamweaver, Adobe Flash va boshqa veb-nashrlarni yaratishga yo'naltirilgan turli instrumental dasturiy vositalardan foydalanish mumkin. Elektron portfelni mazmun bilan to'ldirish ishini tashkil etishda, pedagogik faoliyatda muhim bo'lgan materiallarning to'g'ri tanlovida quyidagi: turli mavzular bo'yicha materiallar berilishi yaxlitligi; aniq tuzilmasi va ti-zimlashtirilganligi; chuqur va sifatli ishlab chiqilganligi; to'g'ri bayon etilishi; tartibli va estetik tayyorlanganligi; doimiy va muntazam yangilanishi; dasturiy-metodik to'plamlar ishlab chiqilishi talablariga muvofiqligi jihatlariga e'tibor qaratish zarur.

«Elektron portfel» mazmunini dasturiy-metodik majmua bilan to'ldirishda ta'lim jarayoniga axborot-kommunikatsiya texnologiyalarini tatbiq etishning muhim yo'nalishlaridan biri o'qitishda kompyuter vositalari: elektron o'quv qo'llanmalari; kompyuterli test topshiriqlari; multimediyali taqdimot va ta'limiy dasturlardan foydalanish bo'lib hisoblanadi. «Elektron portfel»ning eng muhim qismi bo'lgan kompyuterda amalga oshiriladigan ta'limiy vositalarga, ta'lim jarayonini tashkil etishda, fanlarning (psixologiya, pedagogika, informatika va boshqa) so'nggi yutuqlari asosida qurilgan, pedagog kasbiy faoliyati funksiyasining bir qismini amalga oshiruvchi va talabalar bilimlari mazmun-

motiyatini anglash faoliyatlarini interaktiv boshqaruvchi asosiy didaktik talablarga javob beradigan o'quv (ta'limiy) dasturlar kiradi.

Xulosa qilib aytganda, agar har bir OTM o'qituvchisi yaxlit elektron portfelga ega bo'lib, barcha muhim materiallarni jamlasa, ta'lim jarayonini tashkil etishda ahamiyatli bo'lgan didaktik samaradorlikka erishish mumkin. Bundan tashqari, pedagog o'zining elektron portfelidan mustaqil foydalanishi ham, boshqa o'qituvchilarning va IT-texnologiyalari mutaxassislarining eng yaxshi ishlanmalaridan foydalanishlari ham mumkin. Shu tariqa, elektron portfelni yaratish va mazmun bilan uni to'ldirish vaqtida, har bir OTM o'qituvchisi kasbiy mahorati o'sishiga, kompyuter vositasida o'qitishga hamda o'z fani bo'yicha bilim darajasini takomillashtirishga erishadi.

**Nazorat savollari:**

1. Portfolio so'zining ma'nosi nima?
2. Portfolio atamasidan dastlab qayerda va qaysi sohalarda qo'llanilgan?
3. Portfolioning qanday turlari mavjud?
4. www.portfolio.bimm.uz portfolio tizimi qanday qismlardan tashkil topgan?
5. Xorijiy portfolio tizimlaridan qaysilarini bilasiz?

### 3.2. Elektron ta'limni tashkil qilish vositalari

**Reja:**

1. Elektron ta'limni tashkil etish uslublari
2. Masofali o'qitish modellari
3. LMS tizimi – pedagogning shaxsiy, kasbiy axborot maydonini takomillashtirishning vositasi
4. Moodle tizimi – pedagogning shaxsiy, kasbiy axborot maydonini takomillashtirishning vositasi

**Kalit so'zlar:** Eksternet, Forums, Materials, Messenger, Chat, Exercises, Group work, Student tracking, Atutor, Chamilo, OLAT, Content managing, Forums, File



discussions, Quizzes with different kinds of questions,Wikis, Blogs, Podcast, Surveys, Chat, Announcements, Email Archive, Chat Room online, Assignments, Grade book, Module Editor, QTI Authoring, QTI Assessment, Section Management, Syllabus, Forms, Evaluations, Glossary, Matrices, Layouts, Templates, Reports, Wizards, Search, Web Content, WebDAV, Wiki, Site Setup, MySakai, Widgets, Konsorsium model, Franchayzing model, Validasiya model.

#### *Elektron ta'limni tashkil etish uslublari*

1. ***Eksternat turida o'qitish***. Ushbu o'qitish uslubi umumiy ta'lim maktab o'quvchilari va oliygox talabalariga yo'naltirilgan bo'lib, qandaydir sabablarga ko'ra stasionar o'quv yurtiga borolmagan o'quvchi va talaba uchun mo'ljallangan. Masalan, 1836 yili London universitetida qandaydir sabablarga ko'ra ana'naviy o'quv yurtiga bora olmagan o'quvchi va talabaga yordam sifatida u yoki bu darajadagi hujjat(attestat, diplom)ga ega bo'lish uchun imtixon olishga tashkil etilgan. Ushbu vazifa xozirgi kungacha talabalarni stasionar o'qishi bilan birga saqlanib kelmoqda.

2. ***Bir universitet negizida o'qitish***. Bu stasionar o'qimaydigan (on-campus), ya'ni masofadan turib, sirtdan yoki masofali va kompyuterli telekommunikasiyani o'z ichiga olgan yangi axborot texnologiyalari asosida (off-campus) o'qiqtgan talabalar uchun butun bir ta'lim tazimidir. Dunyodagi ko'pgina nufuzli oliygoxlardagi ta'limning turli attestatlarini olish uchun mo'ljallangan dasturlar turli tumandir. Masalan, Avstraliya Janubiy Uelsning yangi universitetida 3000 talaba stasionar holda o'qisa, 5000 ta talabaga sirtqi va masofali ta'lim tizimi orqali o'qitiladi.

3. ***Bir necha o'quv yurtining hamkorligi***. Sirqi va masofali o'qitish dasturini amalga oshirishda qilinadigan hamkorlik ularni, sifatliroq va kam xarajatli bo'lishini ta'minlaydi.

Bunday tajriba, masalan Keprikon universitetlari aro tele o'qitish dasturida amalda qo'llangan bo'lib, unda Boliviya, Braziliya, Chili va Paragvay

universitetlari ishtirok etadi. Ana shunday hamkorlik misoli bo'lib, "Ta'limda hamkorlik" dasturi xizmat qilishi mumkin. Britaniya hamdo'st mamlakatlarining yurtboshilari 1987 yili barcha hamkor davlatlar uchun masofali o'qitish tarmog'ini tashkil etishni kelishib olishga yig'ilishgan. Dasturning istiqboldagi maqsadi - hamdo'st mamlakatlarda mavjud kollej va universitetlar negizida ixtiyoriy ta'lim olish imkoniyatini yaratib berishdan iboratdir.

4. ***Maxsus masofali o'qitish maqsadida tashkil etilgan avtonom ta'lim massasasalari***. Ana shunday muassasalardan eng yirigi Londondagi ochiq universiteti (Thy Open University) hisoblanadi. Hozirgi kunda unda nafaqat Buyuk Britaniya balki ko'pgina hamdo'st davlatlarining talabalari masofadan turib o'qimoqda.

AQShda bunday universitet sifatida Milliy texnologik universitet (Kolorado shtati)i misol bo'lishi mumkin. Bu universitet 40 ta muxandislik kollejlari bilan birgalikda turli mutaxassisliklar bo'yicha xodimlarni tayyorlamoqda.1991 yili universitet shtat raxbariyati va biznes sohasi bilan yaqin hamkorlikda 40 ta kollejni masofali o'qitish tarmog'i bilan birlashtirdi.

5. ***Avtonom o'qitish tizimlari.*** Bunday tizimlar doirasida o'qitish to'la TV va radiodastur, shuningdek, qo'shimcha nashr etilgan qo'llanmalar asosida o'qitmoqda. Masofadan turib o'qitishning bunday misoli sifatida Amerika - samoan televizion loyihasini keltirish mumkin.

6. ***Multimedia dasturi asosida norasmiy integrallashgan (birlashtirilgan) masofali o'qitish***.

Bunday dasturlar qandaydir sabablarga ko'ra maktabni tamomlay olmagan yoshi katta tinglovchilar auditoriyasiga mo'ljallangan.

Bunday loyhalar ushbu dasturga birlashtirilgan rasmiy ta'lim dasturining qismi (masalan, bunday dasturlar Kolumbiyada mavjud) yoki aniq ta'lim maqsadiga maxsus mo'ljallangan (masalan, Britaniyaning savodxonlik dasturi) yoki maxsus salomatlik profilaktikasi dasturiga yo'naltirilgan (masalan, rivojlanayotgan davlatlar uchun) bo'lishi mumkin.



Ta'lim tizimida qo'llaniladigan masofali o'kitish usulining rang barang shakl va modellari mavjud. Ushbu usulning rang-barangligi masofali o'kitish tizimining shakllanishidagi turli shart-sharoitlari bilan bog'liq. U shartlarga:

- geografik sharoitlar (masalan, davlatlar territoriyasining ko'lami, markazdan uzoqda yoki ajralgan xududlarning mavjudligi, iqlimi va boshqalar);
- davlatning kompyuterlashtirilganlik va axborotlashtirilganligining umumiy darajasi;
- davlatda transport va kommunikasiya vositalarining rivojlanganlik darajasi;
- ta'lim sohasida mavjud an'analar;
- masofali o'qitish tizimi uchun ilmiy-pedagogik xodimlarni mavjudligi va shu kabilar kiradi.

YUNESKO institutining 2000 yildagi tahliliy tadqikot materiallarida ("Distance Education for the Information Society: Policies, Pedagogy and Professional Development") keltirilgan masofali o'qitish modellarini keltiramiz:

***Yagonalik modeli***. Ushbu model tashkiliy tuzilishiga ko'ra faqat masofali o'qitishda va "masofali" talabalar bilan ishlash maqsadida tashkil etiladi. O'qitish shunday amalga oshiriladiki, bunda ta'limning kunduzgi shakli zarur bo'lmaydi. Barcha o'qitish masofadan amalga oshiriladi. Ushbu modelda o'qitishda xududiy markazlar bo'lib, ularda talabalar o'qituvchilardan maslahatlar olishi yoki yakuniy imtihon topshirishlari mumkin.

Bunday oliygoxlarda o'qituvchilarga ham talabalarga ham o'quv faoliyatining shakl va uslublarini tanlashda katta erkinlik beriladi. Vaqt va o'quv jadvallariga qa'tiy chegaralar qo'yilmaydi.

Bunday tamoyilida o'qitish Ochiq universitetlarda, masalan, Buyuk Britaniyaning Ochiq universiteti (United Kingdom Open University - http://www.open.ac.uk) da tashkil etilgan.

***Ikkilangan modeli***. Bunday tizimda oliygox kunduzgi talabalarni ham, qisman kunduzgi va qisman masofali dastur asosida o'qitadi. Har ikkalasida ham

dars jadvallari, o'qitish dasturlari, imtihonlari va baholash mezonlari bir xil bo'ladi. Odatda ikkilangan modelni rivojlantirayotgan oliygox kunduzgi talabalar soni masofali o'qiyotgan talabalar sonidan katta bo'lgan ana'naviy oliygoxlardir. Shuning uchun bir universitetning o'zida ikki shaklning birgaligida ko'proq o'zlarida katta o'quv materiallaridan foydalanish imkoniyatiga ega bo'lgan kunduzgi talabalar yutadilar. Bunday oliygoxlarda masofali kurslar har doim ham foyda keltirmaydi, ba'zan u qisman kunduzgi talabalarni o'qitish hisobidan amalga oshiriladi. Bunday holatlarda asosiy urg'u tajribaga, pedagogika va uslubiy innovasiyalar tadqiqotiga va boshqalarga beriladi. Masofali o'qitishning bunday modeli Avstraliyaning yangi Angliya universiteti (University of New England, Australia - http://www.une.edu.au) da tashkil etilgan.

***Aralash model.*** Bu model universitet talabalarini masofali o'qitishning turli shakllarini, aniqrog'i shakllarning integrasiyasini nazarda tutadi. Masalan, kunduzgi shaklda o'qiyotgan talabalar masofali o'qitish kurslarining dasturlaridagilarni yoki ushbu universitetining o'qituvchisi o'qiyotgan kunduzgi kurslari bilan parallel ravishda qisman o'qiydilar. Shuningdek, bu modelda an'anaviy kurslar doirasida virtual seminarlar, taqdimotlar, ma'ruzalar ko'rinishidagi mashg'ulotlar alohida shakllarining birlashmasi bo'lishi mumkin. Universitet axborot va kommunikasiya texnologiyalari vositalari bilan qanchalik yuqori jixozlangan bo'lsa, shunchalik o'qitish shakllari turli-tuman bo'ladi. Integrallashgan bunday kurslar Yangi Zellandiyadagi Massey universitetida (Massey University, New Zealand - http://www.massey.ac.nz) tashkil etilgan.

***Konsorsium model.*** Ushbu model ikki universitetni birlashmasidan iborat. Bunda ular o'quv materiallari bilan almashadilar yoki ba'zi vazifalarni bo'lishib oladilar. Masalan, bir universitet masofali o'qitish uchun o'quv materiallar ishlab chiqaradi, boshqasi virtual o'quv guruhlarini o'qituvchilar bilan ta'minlaydi yoki masofali o'qitish dasturlarini rasmiy akreditasiyasini o'tkazadi. Bunday hollarda universitet butunlay yoki uning alohida markazalari, fakultetlari, xatto ta'lim xizmati bozorida ishlayotgan tijorat yoki davlat tashkilotlari hamkor bo'lishlari mumkin. Konsorsiumlar faqat qattiy markazlashgan boshqarish va yaratilayotgan



ashyolarning mualliflik hamda material xuquqlarini rioya etish shartlaridagina samarali bo'ladi. Kanadadagi Ochiq o'quv Agentligi (Open Learning Agency, Canada - http://www.ola.bc.ca) konsorsiumga misol bo'lishi mumkin.

***Franchayzing model.*** Franchayzing tamoyilida tashkil etilgan masofali o'qitish modelida hamkor universitetlar bir - birlariga o'zlarining masofali kurslarini beradilar. Bunda ta'lim xizmati bozorida o'zini ko'rsatgan qandaydir universitet o'zida ishlab chiqqan kurslarini masofali o'qitishni endigina tashkil qilayotgan va masofali o'qitish uchun o'quv ashyolarini mustaqil ishlab chiqish tajribasiga ega bo'lmagan boshqa oliygox - hamkorlariga o'qitish huquqini berishi mumkin.

Bunday modelning qiziq tomoni shundaki, talabalar o'zlarining universitetida o'qishga yozilib, konsorsiumga kirgan ilg'or oliygox talabasi kabi o'sha hajmda va o'sha sifatda ta'lim xizmatlalariga, o'qishni bitirganlaridan keyin xatto diplomlariga ega bo'ladilar. Bunda ilg'or universitetning barcha atributikalari o'z kuchini saqlab qoladi. Franchayzing modeliga misol sifatida Buyuk Britaniyaning Ochiq universiteti qoshidagi Biznes Maktabi (Open University Business School, Great Britain) va uning Sharqiy Yevropadagi universitetlari bilan aloqasini olish mumkin.

***Validasiya model.*** Masofali o'qitishning juda keng tarqalgan modeli bo'lib, bunda ta'lim muassasalari masofali o'qitish bo'yicha xizmatlarni barcha hamkorlari teng darajada bajarishlari haqida kelishuv imzolab oladilar. Ularning biri diplom validasiyasi, kurs va dasturlarni akreditasiyasini qiladi, rasman tan olinadigan diplom va sertifikatlarni berishga ma'sul bo'ladi, ilmiy darajalar beradi va xokazo. Bosh oliygox (davlat akreditasiyasiga ega bo'lgan taniqli oliygox) va uning xududlardagi ko'p sonli filiallari orasidagi munosabatlar ham shu model asosida tashkil etiladi.

***Uzoqlashtirilgan auditoriyalar model.*** Bu modelda zamonaviy axborot texnologiyasi vositalari faol foydalaniladi. qandaydir oliygoxda o'tkazilayotgan o'quv kurslar, ma'ruzalar yoki seminarlar talabalar yig'iladigan uzoqlashtirilgan o'quv auditoriyalarga sinxron teleko'rsatuv, videoanjuman, radioeshittirish

ko'rinishida telekommunikasiya kanallaridan uzatiladi. Bunda bir o'qituvchi bir vaqtni o'zida talabalarning katta auditoriyasi bilan ishlaydi. Ushbu model bo'yicha

AQSh ning Viskonsin universiteti (Wisconsin University, USA) da, shuningdek, Xitoyning markaziy radio va televedenie universiteti (China Central Radio and TV University) da masofali o'qitish tashkil etilgan.

***Loyihalar model***. Davlat ta'lim yoki ilmiy-tadqiqot dasturi doirasida keng qamrovlik loyihani amalga oshirish uchun mo'ljallangan masofali o'qitish modelidan iborat. Ushbu modelda asosiy ahamiyat o'quv materiallarini ishlab chiquvchi asosiy mutaxasissis xodimlar, masofali kurslarni olib boruvchi o'qituvchilar va olimlar yig'iladigan ilmiy - uslubiy markazga qaratiladi. Markazda ishlab chiqiladigan masofali kurslar u yoki bu davlat (xudud) ning katta auditoriyasiga uzatiladi. Bunday o'qitish vaqtinchali hisoblanib, loyihada mo'ljallangan ishlar bajarilgandan yoki tugagandan so'ng tugatiladi. Bu modelga misol sifatida Afrika va Lotin Amerkasining rivojlanayotgan davlatlarida turli xalqaro tashkilotlar o'tkazgan qishloq xo'jaligi, agrotexnikaning yangi uslublari, ekologiya bo'yicha va sh.k. masofali o'qitish kurslari olish mumkin.

Chet el davlatlari ekspertlarining ma'lumotlariga ko'ra yaqin yillarda insoniyatni yashashi uchun zarur bo'lgan ta'limning minimal darajasi oliy ta'lim bo'ladi. Shunday ekan, ko'p sondagi talabalarni kunduzgi shaklida o'qitish uchun eng rivojlangan davlatlarning ham byudjet mablag'i chidamasa kerak. Shuning uchun ham oxirgi o'n yillikda kunduzgi bo'limlarda o'qiyotgan talabalarga qaraganda noan'anaviy texnologiya asosida o'qiyotgan talabalarning soni tezroq o'smoqda.

O'qitishning noan'anaviy shakliga o'tish tendensiyasi ana shunday texnologiyalarda kadr tayyorlanadigan va ularni qayta tayyorlaydigan ta'lim muassasalarining sonini ko'payishida ham ko'rish mumkin. 1900-1960 yillarda (60 yil mobaynida) ularning soni 79 ta edi,1960-1970 yillarda (10 yil mobaynida) 70 ta, 1970-1980 yillarda (10 yil mobaynida) 187 ta va 1980 - 1995 yillarda (15 yil mobaynida) 700 ta, 1995-2000 yillarda esa, mingdan oshib ketdi (1 - rasm).



Jahonda uzoq vaqtlardan buyon masofali o'qitish tizimini (MO'T) rivojlanish sabablaridan biri ixtiyoriy yerda yashayotgan har bir o'quvchiga ixtiyoriy kollej yoki universitetda ta'lim olish imkoniyatini yaratishdan iborat. Bu "talabalarni bir davlatdan boshqa davlatga jismonan siljishi" konsepsiyasidan "ta'lim ashyolarini almashinish orqali bilimlarni taqsimlash maqsadida ko'plab g'oya, bilim va ta'lim" konsepsiyasiga o'tishni ko'zda tutadi.

***LMS tizimi – pedagogning shaxsiy, kasbiy axborot maydonini takomillashtirishning vositasi***

**LMS/LCMS** tizimlari elektron ta'limni (masofaviy ta'lim jarayonini) tashkil etishning asosiy funksiyalarini o'z ichiga oladi. Bunday funksiyalar qatoriga o'quvchilarning (o'qituvchilarning, kurs yaratuvchi pedagoglarni va boshqalarni) ro'yxatga olish, foydalanuvchilarni o'quv kurslardan chetlashtirish, o'quvchilarning mustaqil ta'lim olish muhitini yaratish, o'quvchi va o'qituvchilarning o'zaro individual yoki guruh bo'lib, hamkorlikda ishlashini (**Web2** elementlarini ishlatish orqali) tashkil etish, guruhlar yaratish va ularni boshqarish, oraliq, joriy va yakuniy nazoratlarni tashkillashtirish va elektron nazorat turlarini yaratish (elektron nazorat turlariga yopiq turdagi test, ochiq turdagi nazorat, moslikni topishga oid, ketma-ketlikni to'g'ri joylashtirish, bo'sh qoldirilgan joyni to'ldirish va boshqa turlari kiradi), har xil turdagi ijtimoiy so'rovlarni tashkillashtirish, o'quvchilarning bilim darajasini monitoring qilish, sertifikatlar (diplomlar) berish imkoniyati, elektron axborot resurslarini (elektron kutubxonalar) tashkillashtirish, elektron o'quv resurslarini eksport/import qilish imkoniyatlari, tizim foydalanuvchilarining (o'quvchilar, o'qituvchilar (tyutorlar), kurs yaratuvchi pedagoglarning) tizimga qachon, qancha vaqt davomida o'quv kontentlar bilan tanishganligi, qaysi **IP**-manzil orqali kirganligini (bu esa qaysi davlatdan tizimga kirganligini aniqlashga yordam beradi), brauzer va qaysi operatsion tizim orqali kirganligi, tizimda mavjud foydalanuvchilarning faolligini maxsus grafiklar orqali monitoring qilish imkoniyati, o'qituvchi (tyutor yoki elektron kurs

yaratuvchi pedagoglar) tomonidan elektron o'quv-resurslarini yaratishi, **Authoring tools**larda **SCORM**, **TinCan** yoki boshqa standartlar asosida yaratilgan elektron o'quv resurslarini yuklashi, o'quvchilarning boshqa o'quvchilar/o'qituvchilar bilan (**Chat**, **Forum**, videokonferensiya, umumiy elektron doskalar yoki tizimning ichki/tashqi xabarlar almashish moduli orqali) muloqotini tashkillashtirish, o'quv jarayonida bo'ladigan yangiliklarni barcha foydalanuvchilarga ommaviy xabar yuborib turuvchi modullarning mavjudligi, iqtisodiy va marketingga oid operatsiyalarni boshqarish va boshqa imkoniyatlarni sanab o'tish mumkin.

Quyida masofaviy ta'lim jarayonini tashkillashtirish imkoniyatini beruvchi erkin va ochiq kodli **LMS** dasturiy majmualarning nomlari va ularning asosiy imkoniyatlari bo'yicha ma'lumotlarni bayon qilamiz:

**Atutor** — Ochiq kodli ta'lim jarayonini boshqaruvchi **LMS** tizimi hisoblanadi. Tizimda mavjud o'qitish modullari: **Forum**s, **Materials**, **Messenger**, **Chat**, **Exercises**, **Group work**, **Student tracking** va boshqa modullari mavjud. Tizim bir necha standartlarni qo'llab-quvvatlaganligi sababli, internet orqali jismoniy nuqsonga ega bo'lgan o'quvchi-talabalar tizim orqali o'quv resurslardan foydalanishlari mumkin. Xususan, ko'zi ojiz talabalar maxsus web-ilovalar orqali tizimga bog'langan holda o'quv kontentdagi so'zlarni audio formatga o'tkazgan holda tinglashi mumkin.

**Chamilo** – tizimi ham boshqa **LMS** tizimlari singari **IMS(IMS Content Packaging, IMS QTI)** va **SCORM** standartlarini qo'llab-quvvatlaydi. Tizim kross-platformali hisoblanib, barcha operatsion tizimlarda ishlaydi. **GPLv3** litsenziyasi asosida ish yuritadi. Bu tizimda kurslarni tashkillashtirishda **sessiya** nomli qo'shimcha moduli mavjud bo'lib, ma'lum kurslar yakuni bo'yicha lokal imtihon aratish imkonini beradi. Shuningdek, hisobot bo'limi orqali esa kurslar, imtihonlar va foydalanuvchilarning holati bo'yicha hisobot yaratiladi. **Chamilo** tizimida modullarning imkoniyatlari yildan-yilga takomillashib bormoqda. Xususan, hozirgi kunga kelib qolgan **LMS** tizimlarida mavjud modullarga qo'shimcha



bo'lgan ochiq muloqot va videokonferensiya tashkil etish hamda taqdimot yaratish imkoniyatlari modullari ishlab chiqildi.

**OLAT (Online Learning And Training)** – tizimni ishlab chiqarish 1999-yil **Syurix** universitetida yaratila boshlangan, 2004-yildan boshlab dastur kodi ochiq kodlikka o'tdi. Hozirga kelib, tizimdan 50 000 ga yaqin foydaluvchi va 50 ga yaqin tashkilot foydalanib kelmoqda. Boshqa **LMS** lar singari **IMS (IMS Content Packaging, IMS QTI)** va **SCORM** standartlarni qo'llab-quvvatlaydi. **OLAT** dasturiy majmuasida mavjud o'quv modullari quyida keltirilgan: **Content managing, Forums, File discussions, Quizzes with different kinds of questions,Wikis, Blogs, Podcast, Surveys, Chat** va boshqa modullari mavjud. **Apache License 2.0** asosida foydalanish mumkin. **OLAT** tizimini ishlatish uchun talab etiladigan dasturiy majmualar: **Java SDK**, **Tomcat Servlet Engine**, ma'lumotlar omboridan **MySQL** yoki **PostgreSQL**. **OLAT** dasturiy majmuasida foydalanuvchilar (administrator, o'qituvchi, o'quvchi) rollaridan foydalanishlari mumkin.

**Dokoes** – **Clarolinening** 1.4.2 versiyasidan ajralib chiqqan yangi dasturiy majmua hisoblanadi. **Dokoes Claroline** platformasini ishlab chiqqan dastlabki ishchi guruh bir necha a'zolarining ish mahsuli bo'lib, ular ta'lim muassasalari uchun yaratilgan **Claroline** tizimidan farqli ravishda, davlat korxonalarining ishchi xodimlariga moslashtirishni maqsad qilishdi va amalga oshirishdi. **Dokoes** dasturiy majmuasining 2 turdagi versiyalari ishlab chiqarilgan, ular **Dokoes Free** – bepul va **Dokoes Pro** – bepul bo'lmagan, qo'shimcha modullarga ega bo'lgan dasturiy paketlaridir. Lekin **Dokoes Free** versiyasi yordamida ta'lim jarayonini tashkillashtirish uchun kerak bo'ladigan barcha o'quv modullari mavjud. Tizimning mavjud o'quv elementlaridan va o'qitish modullaridan ta'lim muassasalarida ham foydalanish mumkin. Hozirgi vaqtda **LMS** larining ko'pchiligi ijtimoiy tarmoqlardagi mavjud g'oya asosida o'zlarining ishchi muhitlarini shunday tarmoqlarga moslashtirmoqda. Shunga ko'ra, bu tizimda ham ijtimoiy tarmoq elementlari keng kiritilgan. Yuqorida keltirilgan **LMS** tizimlari

singari **Dokoes** dasturiy majmuasi ham **SCORM** standartini qo'llab-quvvatlaydi. Bu esa ushbu standartni qo'llab quvvatlaydigan boshqa **LMS** tizimlariga o'quv kurslarini eksport/import qilish imkoniyatini beradi.

**Sakai** – dunyoning ko'pgina ta'lim muassasalarida keng foydalanib kelinayotgan navbatdagi ochiq kodli **GNU GPL** litsenziyasi asosida erkin tarqatiluvchi dasturiy majmua hisoblanadi. Boshqa **LMS** tizimlaridan farqi shundaki, tizim to'liq **JAVA** tilida yozilgan. Shu sababli tizim kross-platformali hisoblanadi. **Sakai** dastur majmuasining o'zida ma'lumotlar ombori mavjud bo'lib, agar foydalanuvchilar soni kam bo'lsa, tizimning ichki ma'lumotlar omboridan foydalanish mumkin. Agar foydalanuvchilar soni ko'p bo'lsa, u holda **MySQL** yoki **Oracle** ma'lumotlar omborida ishlashi mumkin. **Sakai** dastur majmuasida ta'lim jarayonini boshqarish imkoniyatini beruvchi quyidagi umumiy modullar mavjud:

**Announcements** (E'lonlar) – tizim foydalanuvchilariga tegishli e'lonlarni yetkazish uchun xizmat qiladi;

**Drop Box** (Fayllar almashinuvi) - talabalar/o'qituvchilar va o'qituvchilar va talabalar o'rtasida (shaxsiy) hujjatlar almashinuvini ta'minlashga xizmat qiladi;

**Email Archive** (Elektron pochta arxivi) – bu modul orqali tizimdagi foydalanuvchilarning pochta xabarlari tizimning arxiv pochtasida saqlanadi;

**Resources** (Resurslar) – tizim ichidagi foydalanuvchilar o'zlarining o'quv resurslarini saqlashlari va ularni jamoaga e'lon qilish imkoniyati;

**Chat Room online** - ravishda tizim ichidagi foydalanuvchilar o'rtasida aloqani o'rnatish muhiti;

**Forums** – biror-bir mavzu bo'yicha diskussiya mavzularini ochish mumkin;

**Online** muloqotdagi chatdan farqli ravishda bu modul orqali **off-line** ravishda muammoli vaziyatlarni tahlil qilish mumkin;

**Message Center** (Xabarlar markazi) – tizim foydalanuvchilari o'rtasida ichki xabarlar almashish moduli;

**News/RSS** - dinamik yangiliklarini o'zingizning kompyuteringizga eksport qilish imkoniyati;



**Poll tool** (So'rovlar o'tkazish) – tizim ichida har xil so'rovlar o'tkazish imkoniyati;

**Presentation** (Prezentatsiya) bir vaqtning ichida bir nechta foydalanuvchilar uchun fayllarni taqdimot qilish imkoniyatini beruvchi modul;

**Profile/Roster** – tizimda mavjud foydalanuvchilarning shaxsiy profillari bilan ishlash moduli;

**Repository Search** – tizim ichidagi ma'lumotlarni qidirish moduli.

O'qituvchi uchun maxsus ishchi modullari (**Teaching tools**) quyidagilardan tarkib topgan:**Assignments, Grade book, Module Editor, QTI Authoring, QTI Assessment, Section Management, Syllabus.**

Tizim muhitida o'quvchi uchun ishchi modullari (**Portfolio tools**) quyidagilardan iborat:**Forms, Evaluations, Glossary, Matrices, Layouts, Templates, Reports, Wizards, Search, Web Content, WebDAV, Wiki, Site Setup, MySakai, Widgets.**

**Ilias** – bu tizim ham erkin va ochiq kodli masofaviy ta'lim jarayonini boshqaruvchi **LMS** tizimi hisoblanadi. Dasturiy majmua 1998-yildan hozirgi vaqtgacha rivojlanib kelmoqda. Boshqa tizimlarda mavjud bo'lgan o'qitish modullari bu tizimda ham bor: **Forums, Materials, Messenger, Chat, Exercises, Student tracking, Calendar, Glossari, Wiki** va boshqa modullari mavjud. Ushbu **SCORM** standartiga to'liq javob beradi. Tizimning boshqa tizimlarga nisbatan avfzal tomonlaridan biri elektron nazorat turlarining yaxshi yo'lga qo'yilganidadir. Quyida ko'rsatilgan elektron nazorat turlari: **single choice, multiple choice, matching, fill-in-the-blanks, hot spots, flash, java applet** va boshqalarni o'z ichiga oladi. O'quvchilarning olgan natijalarini tahlil qilish va sertifikatlash imkoniyati ham mavjud.

**ATutor** – tizimi ommalashgan masofaviy ta'lim tizimlari qatoriga kiradi. **ATutor** tizimning tarkibida quyidagi modullar mavjud: **Forum, Glossary, File Storage, Site map, My tests and surveys, My tracker, Directory, Export content, Chat, Links, Polls, Blogs, Web search** va

h.k. Bu tizimda yaratilgan kurslar ob'yektga mo'ljallangan dasturlash tillarida klasslarni yaratish jarayoni kabi uch xil tipda aniqlanadi. Chunonchi, **public, Private, Protected**. Foydalanuvchilar bilan ishlashda ham ular uchun bir qancha rollar mavjud bo'lib, ular **disabled** (ta'qiqlangan), **deconfirmed** (faollashtirilmagan), **student** (talaba), **instructor** (o'qituvchi tyutor), **administrator**(administrator).

**Open ELMS** – erkin va ochiq kodli navbatdagi masofaviy ta'lim jarayonini tashkillashtirish imkoniyatini beradigan tizim bo'lib, **GNU GPL** litsenziyasi asosida foydalanuvchilarga foydalanishlari uchun tarqatiladi. Tizimning o'zi erkin va ochiq kodli bo'lganligi bois ham, dasturiy majmuani yaratishda ochiq kodli dasturiy ta'minotlardan foydalanilgan.

**eFront** – dasturiy majmua **PHP** ni qo'llab-quvvatlovchi barcha operatsion tizimlarda ishlaydi. Ma'lumotlar bazasi sifatida **MySQL** va **PostgreSQL** dan foydalanish mumkin. Boshqa **LMS** lar singari **IMS** va **SCORM** standartlarni qo'llab-quvvatlaydi. Tizim 30 dan ortiq tilga tarjima qilingan, shu qatorida o'zbek tilidagi tarjimasi ham mavjud. **eFront** tizimining bir qancha versiyalari ishlab chiqarilgan, ular **Editions, Enterprise, Educational** va **Open-source**. **Open-source** versiyasidan foydalanish bepul hisoblanib, qolgan versiyalaridan foydalanish uchun ma'lum qo'shimcha pul evaziga sotib olishingiz mumkin bo'ladi. Lekin **eFront** dasturiy majmuasining **Open-source** versiyasi masofaviy ta'lim jarayonini tashkillashtirishingiz uchun yetarli hisoblanadi. Mazkur tizimda o'quv jarayonini tashkil etish uchun bir qancha umumiy modullar mavjud ular qatoriga quyidagilar kiradi: **youtube, wiki, workbook, translate, translator, thumbnail, shared files, rss, quote, links, quick mails, lessonstats, lesson sidebar, journal, gradebook, flashcards, faq, crossword, complete test, billboard, banners, blogs, certificates, bbb, chat, infoliosk, idle users, outlook invitation, mg reports** va **administration tools**. Tashkil etilgan darslar uchun quiydagicha maxsus modullar mavjud: **Theory** (Nazariy qism), **Examples** (Misollar), **Projects** (Loyixalar), **Tests** (Testlar), **Lesson rules**



(Dars qoidalari), **Forum** (Forum), **Comments** (Izohlar), **Announcements** (E'lonlar), **SCORM**.

Ko'rinib turibdiki yuqorida ko'rib chiqilgan **LMS** tizimlarining imkoniyatlari bir-biridan qolishmaydi.

***Moodle tizimi – pedagogning shaxsiy, kasbiy axborot maydonini takomillashtirishning vositasi***

**Moodle** – Web muhitida o'qitish va online rejimdagi darslarni tashkil qiluvchi kuchli pedagogik dasturiy majmua hisoblanadi. Mazkur tizimda **Forums**, **Materials**, **Messenger**, **Chat**, **Exercises**, **Group work**, **Student tracking** kabi ko'plab o'qitish modullar mavjud.

Boshqa **LMS**lar singari **IMS**, **SCORM** va boshqa standartlarni qo'llab-quvvatlaydi. Tahlillar shuni ko'rsatadiki, boshqa **LMS** tizimlarga qaraganda, eng ko'p qo'shimcha plagin va modullari mavjud bo'lgan dasturiy majmua bu **Moodle** dasturiy majmuasidir.

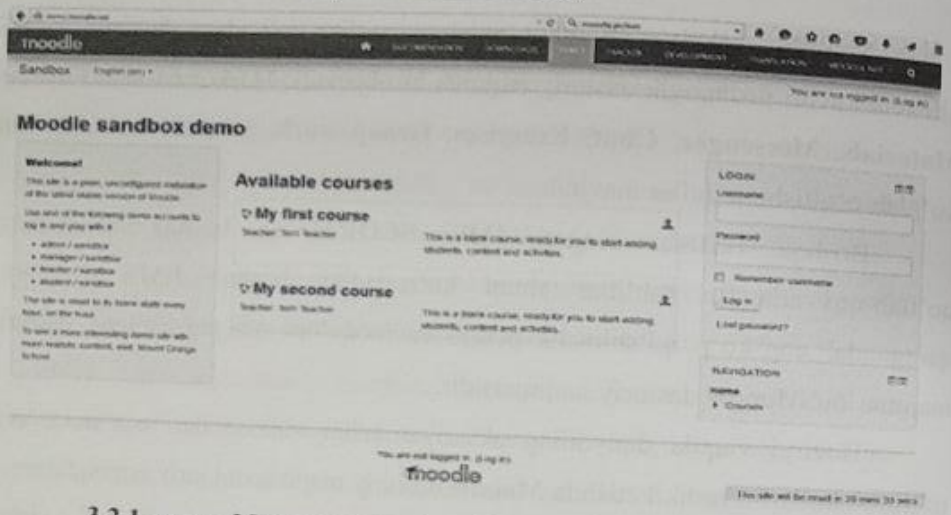
Hozirgi vaqtda dunyoning aksariyat ta'lim muassasalari o'z masofaviy ta'lim tizimilarini tashkil etishda **Moodle** dasturiy majmuasini joriy etmoqdalar.

Shuningdek, Respublikamizdagi ko'plab ta'lim muassaslari virtual ta'lim muhiti sifatida aynan **Moodle** dasturiy majmuasi foydalanib kelinmoqda. Xususan, Toshkent axborot texnologiyalari universitetining "Virtual ta'lim muhiti" (http://etuit.uz), O'zbekiston Milliy universitetining «Ochiq o'quv-axborot markazi», Xalq ta'limi vazirligi qoshidagi «Multimedia umumta'lim dasturlarini rivojlantirish markazi» (http://moodle.uzedu.uz), Toshkent Turin Politexnika universiteti (moodle.polito.uz), Andijon mashinasozlik instituti (http://moodle.andmiedu.uz).

Ochiq kodli **Moodle** dasturiy majmuasi o'quv jarayonini boshqaruvchi **Web** interfeysli muhitga yo'naltirilgan maxsus tizimi bo'lib, asosan global tarmoqda foydalanishga mo'ljallangan. Tizimni yaratishda PHP, MySQL, AJAX, JavaScript, HTML, CSS, XML jQuery kabi qator ochiq kodli dasturiy vositalardan foydalanilgan. Uni ishlatish uchun ma'lumotlar omborini boshqarish dasturi (**MySQL** yoki **PostgreSQL**), **PHP** protsessori,

**Web-xizmati** (**Apache** yoki **IIS**) dasturlari sozlangan server zarur. Operatsion tizim sifatida ixtiyoriy keng tarqalgan operatsion tizimlardan biridan foydalanish mumkin (**Windows, Linux, Mac OS X, Novell Netware**). Mazkur o'quv qo'llanma yozilayotgan vaqtda **Moodle** tizimining **2.9** versiyasidan foydalanilgan. Tizimning rasmiy internet manzili:

http://www.moodle.org




**3.2.1 -rasm. Moodle dasturiy majmuasining umumiy ko'rinishi**

**Moodle** tizimidan foydalanish uchun dastlab mazkur **LMS** tizimida yaratilgan ilovaga a'zo bo'lish talab etiladi. **Moodle** tizimida ro'yxatga olish jarayoni barcha versiyalarida deyarli bir xil kechadi.

Zamonaviy dunyo taraqqiy qilib rivojlanish natijasida kompyuter texnikasi va aloqa vositalari insoniyat hayotini tubdan o'zgartirib bormoqda. Bunday o'zgarishlar ta'lim sohasiga ham o'ziga xos ravishda ta'sir qiladi va o'qituvchi va talabaning masofadan turib o'zaro muloqot qilishi va ta'limning olib borilishi buning yorqin namunasidir. Ushbu qo'llanmada elektron ta'limning uslub va vositalari , ya'ni Moodle elektron kurslari boshqaruv tizimi asosidagi ta'lim tizimi haqida fikr yuritiladi.

Moodle tizimini quyidagi maqsadlarda ishlatish mumkin:



– masofaviy ta'lim uchun- bunda o'qituvchi va talaba ko'p vaqtda yuzma-yuz uchrashmasdan ta'lim olib boriladi;

– ta'limning masofaviy qo'llab-quvvatlanishi-elektron ta'lim vositalari asosida talabalar Moodle tizimidan foydalangan holda topshiriqlarni olishi va uni tekshirish uchun yuborishlari mumkin;

– amaliy topshiriqlarning, testlarning bajarilishi elektron ta'lim tizimi moodleda o'quv mashg'ulotlari vaqtida amalga oshiriladi.

Moodle tizimi quyidagilarni amalga oshirishga imkon beradi:

– o'qituvchi va talabaga ta'lim olish uchun qulay vaqt va joyning tanlash imkoniyatining mavjudligi;

– bilimning puxta o'zlashtirilishi;

– o'qituvchi va talabaning kerak bo'lgan vaqtdagina muloqotda bo'lishi. Agar talaba topshiriqlarni o'z vaqtida bajarib borsa, u o'qituvchi bilan muloqotda bolib boradi.

– ta'limning individualligi;

– vaqt va pulning tejalishi-o'quv mashg'uloti uchun vaqt va pulning sarflanishiga zaruriyat bo'lmaydi.

Moodle tizimida ishlash uchun uni Internetdan yuklab olish kerak. Moodle - masofaviy ta'lim olish tizimi quyidagi bosqichlardan iborat:

Ta'lim berish jarayoniga tayyorgarlik;

Ta'lim berish jarayoni.

Sistemada foydalanuvchi huquqlarini aniqlovchi quyidagi asosiy rollar mavjud:

Administrator- barcha ishni bajara oladigan shaxs;

Kurs yasovchisi (создатель курсов(course creator)) – sistemada kursni tahrirlash, ro'yxatga olish va o'qituvchi tayinlash huquqiga ega;

O'qituvchi (teacher)-o'z kursini tahrirlash va unga assistentlarni, talabalarni tayinlash huquqiga ega;

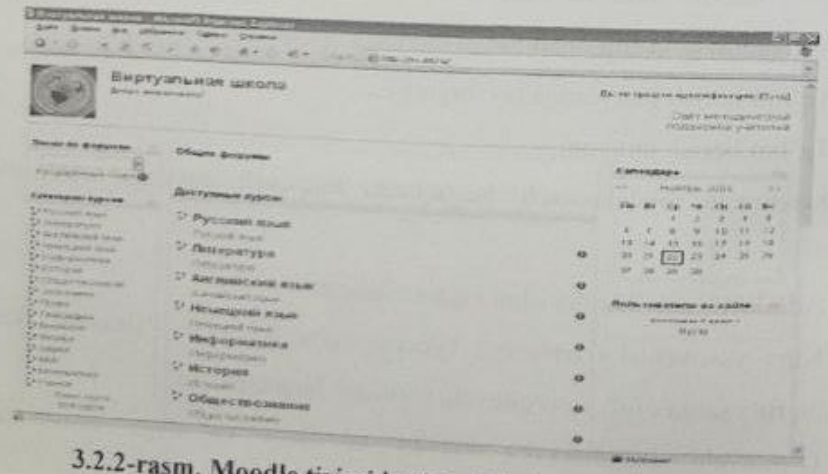
Assistant(non-editing teacher) – kursni tahrirlash huquqiga ega bo'lmagan, ammo talabarning baholarini, kursning topshiriq va test natijalarini kuzatib borish huquqiga ega ;

Student (Student)- O'ziga tegishli bo'lgan kursda ishlash, kurs materiallarini ko'rish, topshiriqlarni tekshirishga yuborish, testlarni bajarish, forum va chatlarda ishtirok etish huquqiga ega;

Gost(guest)- kurs kategoriyalari bilan tanishuvchi menmon sifatida kirish huquqiga ega shaxs.

Administrator tomonidan o'qituvchi registratsiya qilingan(ro'yxatdan o'tkazilgan) bo'lsa unga login va parol belgilanadi. Sistemaga kirish uchun login va parol berilishi zarur.

Moodle tizimi yordamida masofadan turib ta'lim berish jarayoni juda samarali bo'lib, bunda talaba o'zi o'rganayotgan fanning boshlangich qismidan boshlab mustaqil o'rganadi. Har bir ma'ruza turli ko'rinishdagi topshiriq savollari bilan to'ldirib borilgan.Talaba mavzularga doir topshiriqlarni mustaqil ravishda bajaradi va fan bo'yicha olgan bilim, ko'nikmalarini orttirib boradi. Agar biror topshiriqni bajara olmasa u holda ma'ruza qismini qayta takrorlash imkoniyati mavjud.




**3.2.2-rasm. Moodle tizimi bosh sahifasining ko'rinishi.**

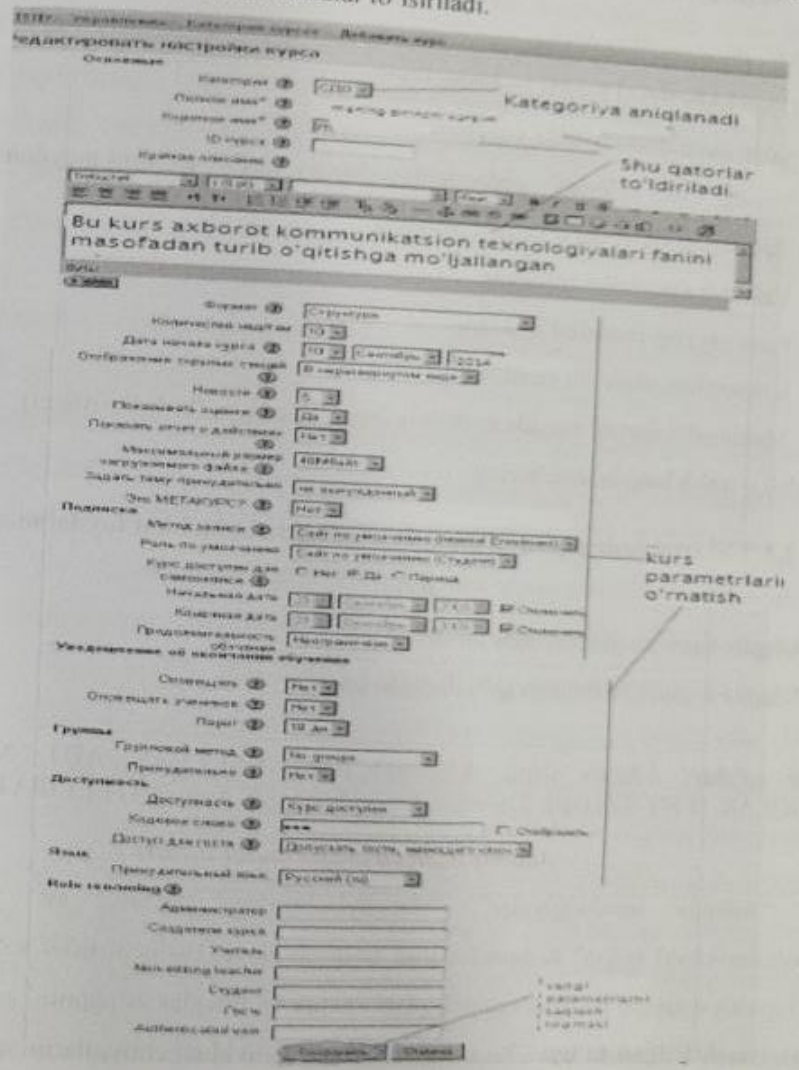
**Yangi kurs qo'shish.** Sistemaga yangi kurs qo'shish huquqiga administrator, kurs yasovchi va o'qituvchi (agarda o'qituvchiga administrator



tomonidan kurs yasash huquqi berilgan bo'lsa) ega bo'ladi. Kursni yasash uchun kurslar kategoriyasi oynasidan kurs qo'shish( **Добавить курс**) bandi orqali amalga oshiriladi.

1.Kurs qo'shish( **Добавить курс**) tugmasi bosiladi.

2.Kurs qo'shish oynasining formasi ekranga chiqadi. Bunda kerakli parametrlar o'rnatilib, kerakli bandlar to'ldiriladi.




**3.2.3-rasm. Kurs qo'shish oynasi.**

Kurs qo'shish oynasida kursning kategoriyasini aniqlash uchun oynadan kurs qaysi kategoriyaga tegishli ekanligi aniqlanadi. Agar darchada yaratayotgan kursga tegishli oyna bo'lmasa u holda ixtiyoriy bir kategoriyani tanlab keyin uni o'zgartirish mumkin.

**Nazorat savollari**

1. Moodle tizimini izohlang.
2. Open LMS tizimi haqida izohlang.
3. Sakai qaysi dasturiy tilde yozilgan.
4. Moodle, LMS tizimlari – pedagogning shaxsiy, kasbiy axborot maydonini takomillashtirishning vositasi haqida izohlang.
5. Validasiya modelini izohlang.
6. Franchayzing modelini izohlang.
7. Konsorsium modelini izohlang.
8. Multimedia dasturi asosida norasmiy integrallashgan (birlashtirilgan) masofali o`qitish haqida izoh bering.

### 3.3. Elektron pedagogikada adaptiv o'qitish tizimlaridan foydalanish

**Reja:**

1. Adaptiv tizim va platformalar turlari
2. Adaptiv o'qitish tizimlarga qo'yiladigan talablar

**Kalit so'zlar:** Adaptiv tizim, AVANTI tizim, PALEVAS, ADT, NASOS, SCHOLAR, WHY tizimlari, Knewton, Smart Sparrow, Aero, INTELLIPATH.

*Adaptiv tizim va platformalar turlari*

"Adaptiv texnologiyalar", "shaxsiylashtirilgan ta'lim" va "adaptiv (moslashuvchan) ta'lim" tushunchalarini farqlash zarur. Birinchi ta'rif sotib olish yoki qurish mumkin bo'lgan raqamli platformalar va ilovalar to'plamini anglatadi. **Shaxsiylashtirilgan ta'lim** - bu o'quvchilarning individual ehtiyojlarini qondirish uchun kursni aniq sozlashga qaratilgan umumiy o'qitish va o'rganish amaliyotidir.



**Adaptiv** (moslashuvchan) **ta'lim** shaxsiylashtirilgan ta'lim shakllaridan biri bo'lib, unda moslashuvchan texnologiyalar muhim rol o'ynaydi.

**Adaptiv** (lotincha **adapto** - moslashtiraman) - har bir o'quvchining tabiiy moyilligi va qobiliyatiga muvofiq intellektual rivojlanishning optimal darajasiga erishishga yordam beradigan o'quv tizimi.

**Adaptiv** (moslashuvchan) **ta'lim** - "har bir o'quvchini jalb qilish uchun samarali va shaxsiylashtirilgan ta'lim traektoriyalarini ta'minlashga qaratilgan shaxsiylashtirilgan ta'limni ta'minlash" uchun mo'ljallangan ta'lim metodologiyasi.

**Adaptiv** (moslashuvchan) **ta'lim** - o'z vaqtida fikr-mulohazalar, yo'llar va resurslar orqali (bir o'lchamli o'rganish tajribasini taqdim etish o'rniga) shaxsning noyob ehtiyojlarini qondiradigan shaxsiylashtirilgan ta'lim tajribasini taqdim etishdir.

Adaptiv – axborotlarni va ulardan foydalanish jarayonini o'rganish hamda o'rgatish uchun qulaylashtirish, moslashtirish asosida kutilgan natijaga erishish.

Masofaviy ta'lim an'anaviy ta'lim turidan quyidagi xarakterli xususiyatlari biri moslashuvchanlik – ta'lim oluvchida o'ziga qulay vaqt, joy va tezlikda ta'lim olish imkoniyati mavjudligidir.

Hozirgi kunda adaptiv o'qitish tizimlarini www muhitida foydalanish va uning imkoniyatlarini kengaytirish borasida bir qator ishlar olib borilmoqda. Avvalambor elektron o'qitish tizimlari uchun hizmat qiluvchi eng sodda elektron darsliklardan tortib, murakkab tuzilmali AO'Tlar borasida ham birmuncha ishlar olib borilmoqda. Web orqali o'qitishni tashkil etishning o'ziga xos tomonlari bo'lib, ularga qisman to'xtalib o'tishimiz mumkin. Web tarmog'ida bir qancha turdagi elektron o'qitish vositalari mavjud bo'lib, birmuncha oldin ommalashgan intellektual o'qitish tizimlari (IO'T) va adaptiv gipermedia tizimlarining davomchilari hisoblanadi. AO'Tlarning ananaviy masalalari IO'T sohasi doirasida tadqiq qilinadi.

Web tizimlar uch guruhga bo'linishi mumkin: adaptiv axborot tizimlari, ular ma'lumotlarni on-line tartibda personallashuvi asosiga quriladi, masalan, AVANTI yoki PUSH [ tizimlarini keltirishimiz mumkin. Adaptiv filtrlovchi tizim

tizimi bo'lib, ular axborot okeanidagi relevant ma'lumotlarni topadi, masalan, if Web yoki WebTagger&trade lami kiritishimiz mumkin. Uchinchi guruhi -adaptiv o'qitish tizimi. AO'Tlar haqida yuqorida bir qator xarakteristikalarni qarab o'tdik.

Ta'lim tizimi ijodiy jarayon hisoblanadi. Ushbu jarayon, avvalo, kompyuterda aks etirilganda o'z maz'mun mohiyatini imkon qadar yo'qotmasligi lozim.

Hozirgi kunda minglab o'qitish jarayoni uchun mo'ljallangan tizimlar yaratilgan bo'lib, ularning umumiy klassifikatsiyasi mavjud emas. Ushbu tizimlarni quyidagi turlarga bo'lish mumkin:

- mashq qildiruvchi (trenajer);
- bilim, malaka va ko'nikmalarni mustahkamlovchi;
- kognitiv o'qitishni dasturlashga yaqin bo'lgan rejimda ishlovchi tushunchalarni o'zlashtirishga mo'ljallangan;
- imitatsion va modellashtiruvchi;
- o'yinli;
- egallangan bilim nazoratini amalga oshiruvchi;
- ma'lumot va axborot bilan ta'minlovchi.

Intellektual tizimlarning o'ziga xos tomoni shundaki, u o'quv jarayonini boshqaradi. Bu jarayonda intellektual tizimlar masalani to'g'ri qo'yilishi, uni yechish usuli to'g'riligi, yechimning optimalligi, muloqot tilini tabiiy tilga yaqinlashtirishni ta'minlashni amalaga oshiradi.

Muloqot jarayonida biror ta'lim oluvchi, xatti-harakati emas, balki yechim qidirishni tashkillashtirish, hatti-harakatlarni rejalashtirish, nazorat usullari va boshqalar muhokama qilinishi mumkin.

O'qitish muhitini tashkil etishda katta etibor o'quvchining tizim bilan munosabatini muvofiqlashtiruvchi qulay vositalarini ishlab chiqish, shu qatorda o'rganilayotgan ob'ekt va jarayonni vizuallashtirish vositalarini ishlab chiqish lozim. Bu yerda vizuallashtirish tushunchasi ostida qo'yilayotgan o'qitish masalarini vizual tarzda akslantirish lozim, ya'ni masala maksimum hayotga



yaqinlashtirilgan holatga erishilishi tushuniladi. Bu vositalarni o'quvchi (foydalanuvchi) interfeysi nomi bilan umumlashtirish mumkin.

Ilg'or axborot texnologiyalari yutuqlaridan foydalangan tarzda qilingan elektron qo'llanmalar an'anaviy bosma o'quv qo'llanmalari o'rnini bosish barobarida o'qituvchiga aloqador masalalarni ham yechish imkoniyatiga ega.

Matnni muloqot yordamida imitatsiyalab sintezlash, multimedia effektlari bilan boyitish orqali BO bilim olishida qulayliklar yaratuvchi pedagogik kompleks hosil qilinadi.

Bundan tashqari elektron qo'llanmalar BO uchun qulaylik – uning xohlagan tezlik bo'yicha dars tashkil etiladi. Shu qatorda tizim BOning tayyorgarligini, o'qishda ulgurish darajasini qadamba-qadam nazoratini amalga oshirib boradi.

Bunday nazorat o'quvchi uchungina zarur bo'lib qolmay, balki tizim uchun BO modelini qurish imkonini beradi. Bu jarayonda foydalanuvchi o'zi kompyuterda ishlashi jarayonida o'zi erishayotgan yutuq va kamchiliklarni kuzatib turadi.

O'qitish tizimlarining ko'pgina klassifikatsiyasi mavjud bo'lib, ular tizimning maqsad va vazifasiga, ish rejimiga qarab quyidagi turlarga bo'linadi :

- illyustratsiyalovchi;
- maslahat beruvchi;
- operatsion muhit;
- trenajerlar;
- nazoratli o'qitish.

Shu o'rinda bir qator kompyuter o'qitish tizimlarini qarab o'tamiz.

AOS-VUZ [49], ADONIS [7] o'rgatuvchi tizimlari quyidagi sxema asosida ishlatiladi. O'quvchiga o'quv materialidan parcha (bir soatlik dars hajmida) beriladi. Bu material o'zlashtirilganini tekshirish maqsadida bir necha savollar beriladi. Agar javob qoniqarli bo'lsa, keyingi o'quv materiali parchasi namoyish qilinadi.

AVS tizimi ko'p maqsadli mualliflik tili bo'lib, u axborot – ma'lumot, modellovchi va o'rgatuvchi dastur tizimini amalga oshiradi. U uch o'zaro aloqador ekspert tizimlari ko'rinishidagi ekspert-o'qituvchi tizimini qurish imkonini beradi:

- fan sohasini modellashtirish;
- BO modelini yaratish;
- o'qitishni boshqarish.

AVS tizimida fan sohasi freym tarmoq bilimlar modeli ko'rinishida berilgan bo'lib, undagi har bir tugun o'rganilayotgan tushuncha haqidagi axborot bilan bog'liq. Fan sohasi modelining bunday strukturasi Ushbu dasturiy ta'minot muhitida turli darajadagi dasturiy tizim qurish uchun bilimlardan foydalanishda saqlashning, ko'p darajalilikning va davomiylikning universal ko'rinishidan foydalaniladi. AVS tizimi fan sohasi bo'yicha bilim olishning bosqichma – bosqich formasini asosiy uslub sifatida olgan. Lekin AVS murakkabroq bo'lgan alternativ o'qitish uslubini amalga oshiruvchi BO modelini qurish jarayonini ishlata olmagan.

ASOLIYa intellektual o'qitish tizimi chet tili leksikasini o'rgatish uchun mo'ljallangan bo'lib, unda parametrik va strukturaviy moslanuvchi BO modeliga asoslangan navbatdagi o'quv materiali bo'lagini hisoblash uchun qo'llaniladi. Bu yerda o'quv materiali bo'lagi deganda navbatdagi qadamni eslab qolishga mo'ljallangan so'z yig'indisi nazarda tutiladi. Maqsad funksiyasi BO modelida saqlanuvchi o'rganilayotgan elementni bilish yoki bilmaslik bahosiga bog'liq. Optimallik masalasi yechiladi va olingan natija o'qitish ssenariyasi sintezi uchun foydalaniladi. Shuni eslatib o'tish lozimki, ushbu tizimdagi apparat tor ixtisoslik uchun yuqori samaradorlik hisoblanib, universal xarakterga ega emas.

Kadis tizimi o'zida avtomatlashtirilgan o'qitish tizimlarini jamlagan. U mustaqil bilim olishga mo'ljallangan. Kadis tizimining instrumental vositasi o'ngga yaqin turli ssenariyni amalga oshirish imkonini beradi.

PALEVAS/I adaptiv o'qitish tizimlari qurish texnologiyalari asosida bir qator intellektual o'qitish tizimlari: PALEVAS, ADT, NASOS kabilar ishlab chiqildi.



Bulardan PALEVAS mantiqiy dasturlash asoslarini o'rgatishga yo'naltirilgan, ADT tizimi sun'iy intellekt sohasida yuqori malakaga ega mutaxassislarga mo'ljallangan bo'lib, u teoremalarni isbot qilish ko'rinishlariga ega. NASOS tizimi kon uskunalari nosozligini qidirish bo'yicha o'rta mahsus ma'lumotli mutaxassislar tayyorlashga mo'ljallangan.

Ko'rsatib o'tilgan tizimlar mavjud BO, o'rganilayotgan soha va o'qitish uslubiga oid bilimlar asosida turli toifali foydalanuvchilarning individual ta'lim olishini ta'minlaydi.

To'rt darajali BO modeli qo'llaniladi:

- lokal, BO tomonidan oxirgi bajarilgan vazifa ma'lumotni o'zida mujassamlashtirgan;
- joriy, o'zida joriy dars natijasi taxlilini mujassamlashtiruvchi;
- global, kurs bo'yicha o'quv va tarmoq uzellarini bosib o'tish ketmaketligi natijalarini mujassamlashtiruvchi;
- tekshiruv, aprior tekshiruv natijalarini mujassamlashtiruvchi.

Bu tizim tartiblangan ketma-ketlik asosida qurilgan. Biroq PALAVES, ADT, NASOS tizimlarida BO uchun individual vizual axborot mavjud emas.

Yuqoridagi tizimlar qatori intellektual tizim hisoblangan hozirda klassik bo'lib qolgan tyutor tizimlar SCHOLAR, WHY tizimlaridir. SCHOLAR tizimi 1970 yilda taklif qilingan bo'lib, u talabalarga Janubiy Amerika geografiyasini o'rgatishga mo'ljallangan.

Ushbu tizimda mantiqiy xulosa chiqarish mexanizmidan foydalanilgan bo'lib, unda ilk bora fan sohasini modellashtirishda semantik tarmoqdan foydalanilgan.

80–yillarning boshlarida Stiven hamda Kollinz tomonidan ishlab chiqilgan WHY intellektual tyutor tizimida ilk bora «nokompyuter» o'qitish strategiyasi (Suqrot uslubiga asoslangan)ning kompyuter versiyasi amalga oshirishga urinish qilingan. WHY OO'Yu talabalari uchun uslubiyatni o'rgatishga mo'ljallangan tizim. Bu yerda muloqotli rejim asosida malaka, ko'nikma berish maqsad qilib olingan.

WHY tizimi fan sohasini modellashtirishda ssenariylashgan-yo'naltirilgan uslubga asoslangan. Mualliflarning fikricha, u, birinchidan, ssenariylashtirilgan interaktiv jarayon va ikkinchidan o'rganilayotgan fan sohasining mental modeli (mental model)ni izohlab berish uchun yaroqli deyilgan.

Xorijiy intellektual adaptiv platformalar orasida Loud Cloud, Blackboard, Knewton, RealizeIT, Geekie, Smart Sparrow va boshqalar mashhur.

**Knewton** ta'lim xizmati (platforma) 2008 yildan beri o'rganishni shaxsiylashtiradi.

Knewton - moslashuvchan dasturlar va ilovalar ishlab chiqiladigan platforma. Arizona, Alabama, Nevada va Las-Vegas universitetlari kabi yirik ta'lim muassasalari Knevton algoritmlaridan foydalanishlari ajablanarli emas. Knewton platformasining algoritmlari nafaqat AQSh, balki Yevropaning yirik universitetlari tomonidan qo'llaniladi.

Ko'p yillik mehnat va turli tajribalar natijasida Knewton jamoasi universal algoritmlarni yaratishga va talabalar taraqqiyoti haqidagi ma'lumotlarni to'plash, tahlil qilish va ulardan foydalanish uchun keng infratuzilmani rivojlantirishga muvaffaq bo'ldi, jumladan:

1. Bir vaqtning o'zida bilimlar haqida, ma'lum tushunchalarni o'zlashtirish darajasi haqida batafsil ma'lumot to'playdigan ma'lumotlarni yig'ish tizimi.

2. O'quvchining o'ziga xos xususiyatlari va uning ta'limdagi o'zgarishlarga bo'lgan munosabati to'g'risida to'plangan ma'lumotlarga asoslanib, ma'lumotlarni umumlashtiradigan va mazmun parametrlarini mos ravishda to'g'rilashni amalga oshiradigan xulosalar tizimi.

3. Butun tizim ma'lumotlari asosida talabaning imkoniyatlarini baholovchi, buni hisobga olgan holda maqsadlarni rostlaydigan va har bir talaba uchun optimal ta'lim strategiyasini shakllantiradigan shaxsiylashtirish tizimi. Shu bilan birga, shaxsiylashtirish tizimi o'quvchilarning muvaffaqiyati (ish tezligi, maqsadga erishish ehtimoli va boshqalar) haqida tahliliy bashorat qiladi va ta'limning barcha darajalarida shaxsiy statistikani yuritadi.



Avstraliya interaktiv va moslashtirilgan o'quv kurslarini yaratish uchun **Smart Sparrow** ochiq o'quv platformasidan foydalanadi.

Platforma veb-paket bo'lib, keyingi savolni aniqlash uchun faqat eng so'nggi talabalar javoblarini (tanlovlarini) tahlil qiluvchi algoritmlardan foydalanadigan "kichik ma'lumotlar" yondashuviga asoslangan.

O'qituvchi savolga javob berish qiyin bo'lganida, so'rov urinishlari soni yoki harakatsizlik vaqtini o'zgartirganda, talaba bilan o'z vaqtida ko'rsatmalar (video, grafik yoki qo'shimcha material) shaklida fikr-mulohazalarni o'rnatish imkoniyatiga ega.

**Aero** - bu kollej talabalari uchun mo'ljallangan moslashtirilgan raqamli o'quv platformasi. Aero kurs maqsadlari, topshiriq mavzulari va testlarni belgilaydi. Dastur juda katta hajmdagi ma'lumotlarni to'playdi, jumladan, nafaqat savollarga javoblar, balki talabalar topshiriqlarni (nazariyani) qanchalik tez-tez ko'rganligi, qaerda va nimani tanlaganligi haqida ma'lumot.

Dastur qachon va qaysi mavzudan materialni takrorlash zarurligini aniqlashga qodir. O'qituvchi guruhda o'qitishni individuallashtirish, talabalarning bilimlari asosida ma'ruzalarni rejalashtirish imkoniyatiga ega. Natijada, o'qituvchi imtihondan muvaffaqiyatli o'tish yoki materialni o'zlashtirishni bashorat qilish imkoniyatiga ega.

**INTELLIPATH** moslashuvchan o'quv platformasi:

- o'qituvchilarga real vaqt rejimida nafaqat o'quvchilarining mazmun bilan o'zaro munosabatda bo'lgan yutuqlari, balki o'quv materialini qay darajada o'zlashtirganliklari (yoki hali o'zlashtirmaganligi) to'g'risidagi ma'lumotlarni taqdim etish;

- avtomatik ravishda fikr-mulohaza va baholashni yaratadi.

***Adaptiv o'qitish tizimlarga qo'yiladigan talablar***

Moslashuvchan ta'lim texnologiyasi uchun zarur bo'lgan murakkablik darajasi texnologiyaga asoslangan ta'lim yechimlarini ko'pincha uchinchi tomon ta'lim texnologiyalari provayderlari tomonidan ishlab chiqilishi va qo'llab-quvvatlanishiga olib keldi.

Moslashuvchan kurs dasturining ikkita asosiy turi mavjud:

- ochiq tarkibga ko'proq e'tibor qaratadigan va o'qituvchilarga o'z mazmunini yaratish, o'z o'quv maqsadlarini yaratish va o'z darslari ketma-ketligini sozlash imkonini beradigan;

- ikkinchisi, qaysi biri yopiqroq, mazmunga asoslangan bo'lib, kurs mazmuni, baholash va o'rganish maqsadlari platformaga qattiq kodlangan va o'qituvchilar uchun moslashtirish imkoniyatlari cheklangan.

Birinchi tur ko'pincha kichikroq boshlang'ich provayderlar bilan bog'liq bo'lsa, ikkinchi tur ko'pincha darslik nashriyotlari bilan bog'liq, garchi bu har doim ham shunday emas. Ushbu ikki tur o'rtasida keng ko'lamli ta'lim echimlari mavjud bo'lib, ularning ko'pchiligi kursni o'tashdan oldin ba'zi darajadagi moslashtirishga imkon beradi yoki talab qiladi.

Moslashuvchan texnologiyalardan foydalangan holda Avstraliya ochiq ta'lim platformasi Smart Sparrow metodologiyasi texnologiyani talabalarga moslashtirishning ikkita asosiy mexanizmini belgilaydigan ushbu nuqtai nazarga mos keladi:

- rivojlangan moslashuvchanlik;

- algoritmik moslashuv.

moslashtiruvchi usul, bunda o'qituvchi o'z o'quvchilarini tarkibni o'zlashtirishga yo'naltirish uchun ekspert o'rganish ketma-ketligini ishlab chiqadi. Ushbu ekspert modeliga asoslangan moslashuvchanlik yondashuvi texnologiyaga noyob vaziyatlarda qanday munosabatda bo'lish kerakligini aytadi - "Agar BU, keyin" yondashuvi. U kerakli tuzatishlar kiritish, kengaytirilgan tarkibni eng yaxshi ijrochilar bilan baham ko'rish, odamlarni mukofotlash va boshqalar uchun ishlatilishi mumkin. Bu mexanizm o'qituvchiga ko'proq tanlash erkinligini va talaba nimani boshdan kechirayotganini nazorat qilishni ta'minlaydi.

Moslashuvchan ta'lim tizimlari: bo'ronga bardosh berish Lou Pugliese maqolasida aqlli moslashuvchan ta'lim tizimlarining o'ziga xos belgilari keltirilgan:



- qo'lda o'qitish jarayonlari sonini kamaytiradigan avtomatlashtirilgan jarayonlarni yaratish qobiliyati;

- malaka va malakalarning izchil rivojlanishini yaratish qobiliyati;

- tezroq va uzluksiz baholash uchun nazorat, diagnostik va formativ baholash kombinatsiyalaridan foydalanish, ma'lumotlarni to'plash, hisoblash va baholash qobiliyati;

- o'qitish va o'qitish siklida doimiy va barqaror teskari aloqani shakllantirish uchun xulosalar natijasida ma'lumot va ma'lumotlarni o'z-o'zini tartibga solish qobiliyati.

**Nazorat savollari**

1. Adaptiv tizim va platformalar turlari haqida izoh bering.
2. Web tizimlar necha guruhga bo'linadi va ular qanday?
3. O'qitish tizimlari qanday turlarga bo'linadi?
4. O'qitish tizimlarining ko'pgina klassifikatsiyasi mavjud bo'lib, ular tizimning maqsad va vazifasiga, ish rejimiga qarab qanday turlarga bo'linadi?
5. ASOLIYA intellektual o'qitish tizimi nimani o'rgatish uchun mo'ljallangan?
6. PALEVAS adaptiv o'qitish tizimlari qurish texnologiyalari asosida bir qator intellektual o'qitish tizimlarini ishlab chiqildi va ular qanday tizimlar?
7. Individual ta'lim olishda qanday modellar qo'llaniladi?
8. Knewton ta'lim xizmatini izohlang.
9. Adaptiv o'qitish tizimlarga qo'yiladigan talablar

### 3.4. Adaptiv o'qitish tizimlari va flipped classroom texnologiyasi

**Reja:**

1. Flipped classroom haqida
2. Flipped classroom texnologiyasi

**Kalit so'zlar:** Flipped classroom, Adaptiv o'qitish tizimlari

O'zgartirilgan sinf modeli aralash ta'limning bir turidir.

**O'zgartirilgan sinf** (dars) - o'qituvchi uyda mustaqil o'rganish uchun material beradigan o'qitish modeli, yuzma-yuz darsda esa materialni amaliy mustahkamlash mavjud. Flipped learning vodkastlar, podkastlar va oldindan vodkastlardan foydalanish bilan tavsiflanadi. Tafsilotlarga kirishdan oldin, keling, asosiy tushunchalarni tushunaylik.

**Podkast** - bu ovoz fayli (audio ma'ruza), uni yaratuvchisi Internet orqali obuna orqali yuboradi. Qabul qiluvchilar podkastlarni statsionar va mobil qurilmalariga yuklab olishlari yoki onlayn ma'ruzalarni tinglashlari mumkin.

**Vodcast** (talab bo'yicha videodan, ya'ni talab bo'yicha video) podkast bilan taxminan bir xil, faqat videofayllar bilan.

**Pre-vodcasting** - bu maktab o'qituvchisi yoki universitet professori o'z ma'ruzasining vodcastini tuzadigan ta'lim usuli bo'lib, talabalar ushbu mavzu ko'rib chiqiladigan darsdan oldin ham mavzu haqida tasavvurga ega bo'lishlari uchun. Pre-casting usuli teskari sinf usulining asl nomidir.

O'quv jarayonida maxsus dasturlardan foydalangan holda vodkastlardan foydalanish texnologiyasi mavjud:

**CMS** (Content Management System, kontentni boshqarish tizimi) - o'quv materiallari mazmunini yaratish va boshqarish uchun foydalaniladi;

**LMS** (Learning Management System, masofaviy ta'lim tizimi) - o'quv materiallariga kirishni ta'minlaydi, qayta aloqa va gorizontal aloqalarni tashkil qiladi va hokazo.

**Flipped Class** - bu o'rganish modeli bo'lib, unda uy vazifasini bajarish, jumladan, vodcast texnologiyalaridan foydalanishni o'z ichiga oladi:

- video ma'ruza tomosha qilish;
- o'quv matnlarini o'qish, tushuntirish chizmalarini ko'rish;
- mavzuni dastlabki o'zlashtirish uchun testlardan o'tish.

Sinf ishi murakkab nazariy qism va uy vazifasini bajarish jarayonida talabalarda paydo bo'lgan savollarni tahlil qilishga bag'ishlangan (vaqtning 25-30% dan ko'p bo'lmagan). Shuningdek, sinfda o'qituvchi rahbarligida talabalar amaliy masalalarni hal qilishadi va tadqiqot ishlarini bajaradilar. Uyda sinfda darslardan



so'ng amaliy topshiriqlar bajariladi, o'tilgan mavzuni tushunish va mustahkamlash uchun testlar o'tkaziladi.

Agar an'anaviy o'qitishda o'qituvchi nazariyani sinfda tushuntirsa va o'quvchilar mashqlar yoki amaliy mashg'ulotlar olib borishsa, ushbu nazariyani qo'llaydilar. **O'tkazilgan sinf yoki o'girilgan sinf - bu tadqiqot olib boradigan va sinf ichida amaliy mashg'ulotlar uchun material tayyorlaydigan talabalar jamoasi.**

Ushbu modelda harakatlar sarmoyalangan, **nazariyani o'rganadigan va keyin uni darsda qo'llaydigan talabalar.** O'tkazilgan sinf xonasi yaxlit yondashuvga asoslangan. Bir tomondan, to'g'ridan-to'g'ri o'qitish konstruktivistik metodlar bilan birlashtirilib, talaba o'z bilimlarini shakllantiradi va o'qituvchi uyda o'rganish uchun tarkib yaratuvchisidir. Shuningdek, u sinfda qo'llab-quvvatlovchi va nazoratchi vazifasini bajaradi.

Ushbu usulning kamchiliklaridan biri bu sinfdan tashqarida ishlashda **texnologiyalardan foydalanish talab qilinadi.** Shu sababli, raqamli bo'linish tufayli talabalar va ularning bilimlari o'rtasida bo'linish bo'lishi mumkin. O'qituvchilar va talabalar AKTdan foydalanish bo'yicha bilimlarga ega bo'lishlari shart.

### *Flipped classroom texnologiyasi*

Har qanday ota-ona o'qituvchilardan o'z farzandiga individual yondashishni, nafaqat bilim olishga, balki unga xos bo'lgan shaxsiy va ijodiy rivojlanish imkoniyatlarini ochib berishga yordam berishini xohlaydi. Talaba bilan individual ishlashda yoki kichik guruh talabalari bilan ishlashda individual yondashuv aniq va juda oddiy. Ammo darsda butun sinf bilan ishlashda individual yondashuvni qanday amalga oshirish kerak? Moslashuvchan ta'lim texnologiyasi ushbu muammoni hal qilish uchun mo'ljallangan.

Texnologiyaning o'zi esa o'quv jarayoniga moslashuvchanlikni beradi - har bir o'quvchining xususiyatlariga moslashish qobiliyati.

Ushbu texnologiyaning vazifalari mustaqil ishlash va o'z-o'zini nazorat qilishni o'rgatish, bilimlarni mustaqil egallash uchun mashqlarni shakllantirish,

individual xususiyatlariga moslashtirishdir.

Texnologiyaning mohiyati shundan iboratki, darsda o'qituvchi ...

- barcha talabalarning mustaqil ishlarini boshqaradi;
- har bir talaba bilan individual ishlaydi;
- iloji bo'lsa, barcha talabalarni individual ishlarga jalb qiladi;
- o'quv topshiriqlarini va ularni bajarish vaqtini farqlash orqali o'quvchilarning har birining individual xususiyatlarini hisobga oladi; masalan: ko'proq qobiliyatga ega bo'lganlar murakkabroq vazifalarni mustaqil ravishda bajaradilar yoki topshiriqni ertaroq bajarishni boshlaydilar (o'qituvchi qolganlari bilan bajarish usulini ishlab chiqayotganda) yoki uni tezroq bajarish.

Moslashuvchan ta'lim turli xil aniq belgilangan va yaxshi sinovdan o'tgan model va jarayonlarga asoslanadi. Moslashuvchan ta'lim tizimlaridagi ma'lumotlar fan sohasi haqidagi bilimlarni ifodalash va o'quv jarayonida o'quvchilarning xatti-harakatlarini modellashtirish uchun zarurdir.

Ushbu ma'lumotni uchta asosiy modelga bo'lish mumkin: domen modeli, talaba (yoki talabalar guruhi) modeli va moslashish modeli.

**Flipped Class** - bu o'rganish modeli bo'lib, unda uy vazifasini bajarish, jumladan, vodcast texnologiyalaridan foydalanishni o'z ichiga oladi:

video ma'ruza tomosha qilish;

o'quv matnlarini o'qish, tushuntirish chizmalarini ko'rish;

mavzuni dastlabki assimilyatsiya qilish uchun testlardan o'tish.

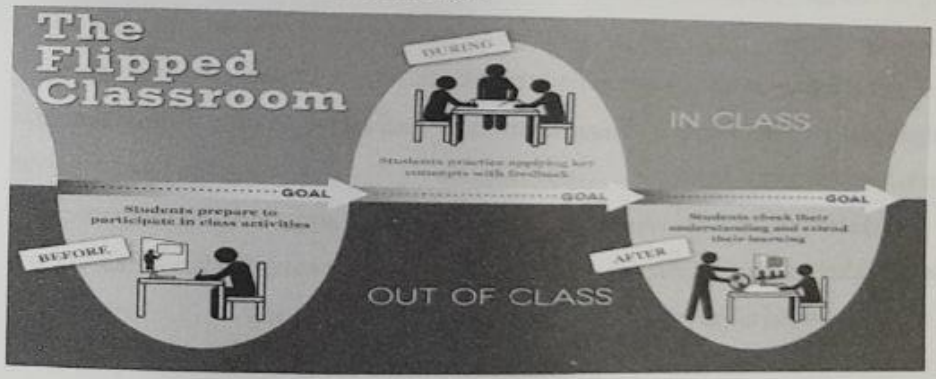
**Flipped Class** - bu pedagogik model bo'lib, unda ma'ruzalarning tipik taqdimoti va uy vazifalarini tashkil etish teskari bo'ladi. Talabalar kafedra yoki o'qituvchining veb-saytida joylashtirilgan ma'ruzalarni o'qiydilar, mavzu bo'yicha barcha materiallarni - taqdimotlarni (masalan, youtube dan qo'shimchalar), ma'lumotnoma va tarqatma materiallarni tomosha qiladilar, darsda esa mashg'ulotlarni bajarish uchun ajratilgan vaqt ajratiladi, mavzular, loyihalar va munozaralarni muhokama qilish. tushuncha



Flipped ta'lim faol o'rganish, o'quvchilarni umumiy faoliyatga jalb qilish, qo'shma ta'lim tizimi kabi g'oyalarga asoslanadi.

O'zgartirilgan sinf xonalarining ahamiyati - talabalar ma'ruza mazmunini muhokama qilishlari, o'z bilimlarini sinab ko'rishlari va amaliy mashg'ulotlarda bir-birlari bilan muloqot qilishlari mumkin bo'lgan guruh mashg'ulotlari uchun dars vaqtidan foydalanish imkoniyatidir. O'quv mashg'ulotlari davomida o'qituvchining roli o'quvchilarni mustaqil izlanishga va birgalikda ishlashga undaydigan trener yoki maslahatchi sifatida harakat qilishdir.

Sinf ishi murakkab nazariy qism va uy vazifasini bajarish jarayonida talabalarda paydo bo'lgan savollarni tahlil qilishga bag'ishlangan (vaqtning 25-30% dan ko'p bo'lmagan). Shuningdek, sinfda o'qituvchi rahbarligida talabalar amaliy masalalarni hal qilishadi va tadqiqot ishlarini bajaradilar. Uyda sinfda darslardan so'ng amaliy topshiriqlar bajariladi, o'tilgan mavzuni tushunish va mustahkamlash uchun testlar o'tkaziladi.




**3.4.1- rasm. Flipped Classroom modeli**

Qaytarilgan sinf modeliga o'tish o'qituvchi rahbarligidan o'quvchi rahbarligiga o'tishdir. Chet el adabiyotida bu o'tish majoziy ma'noda o'qituvchi rolining "sahnadagi donishmand" dan "yondagi gid" ga o'zgarishi sifatida tasvirlangan, uni "dono odam va o'yinchi" dan o'tish sifatida erkin tarjima qilish mumkin. quvur" ga "yo'lboshchi - u boshqaradigan tomondan".

o'qituvchi - Jonatan Bergman va Aaron Sams hisoblanadilar, ular 2007 yilda birinchi marta darslarni tez-tez o'tkazib yuboradigan sportchilarga o'z ma'ruzalarini qanday berishni aniqladilar va keyin bu g'oyani yangi ta'lim yo'nalishiga aylantirdilar. Bunda ularga Amerikaning yirik gazeta va jurnallaridagi nashrlar yordam berdi.

21-asrda teskari sinf modelining roli. Hayotning barcha jabhalarida ro'y berayotgan o'zgarishlar ta'lim tizimiga qiyinchilik tug'diradi, undan "dastlab turish"ni talab qiladi. Ushbu muammoga javob berish uchun siz o'quv jarayoni ishtirokchilari qanday talablarga javob berishlari kerakligini tushunishingiz kerak - ham o'qiydiganlar, ham o'qiydiganlar. Bunday talablarga misol qilib Xalqaro Ta'lim Texnologiyalari Jamiyatining standartlarini keltirish mumkin.

Talabalar uchun yangilangan standart (avvalgisi 2007-yilda, yangisi 2016-yilning iyun oyida nashr etilgan) to'g'ridan-to'g'ri teskari sinfda o'qitish bilan bog'liq bo'lgan ko'plab talablarni o'z ichiga oladi. Ulardan ba'zilari quyida keltirilgan:

Talabalar o'quv jarayonida texnologik vositalardan foydalanishlari, shuningdek, "bilimni chuqurlashtirish uchun o'quv maydonini shaxsiylashtirishlari" kerak.

Talabalar raqamli dunyoda o'rganishning o'ziga xos xususiyatlarini tushunishlari va faqat xavfsiz va qonuniy yo'llar bilan harakat qilishlari kerak.

Materialni o'rganishda talaba tanqidiy fikr yuritishi kerak.

Mavjud materiallarni o'rganish emas, balki "yangi yechimlarni yaratish orqali muammolarni hal qilish" ham muhimdir.

Nima qilish mumkin va nima qilish kerak:

1. O'quvchilaringiz uchun darsdan tashqari foydalanishlari mumkin bo'lgan video taqdimotlar ko'rinishidagi mualliflik materiallarini ishlab chiqing. Albatta, tasdiqlangan dastur doirasidagi ma'lumotlar bilim olish uchun asos bo'lib xizmat qilishi kerak, ammo maktab o'quvchilari o'z o'qituvchisining shaxsiy hissasini ancha yuqori baholaydilar.



2. Ta'lim jarayonini boshqarish tizimlaridan biri foydasiga tanlov qilish va tanlangan tizimga amal qilish. Siz Edmodo o'quv saytidan foydalanishingiz mumkin, uning funksionalligi sizga topshiriqlar berish va bajarilgan ish matniga sharhlar berish imkonini beradi. Talabalar ushbu resursdan juda mamnun, chunki u o'zaro platformali va o'quv materiallari va kutubxona resurslaridan foydalanishni qo'llab-quvvatlaydi.

3. Vazifalar uchun juda aniq muddatlarni belgilang. Ammo ehtiyot bo'ling: agar siz faqat sanani eslatib o'tsangiz, talabalar oxirgi muddatni o'sha kuni yarim tun deb talqin qilishlari mumkin! "Keyingi safar o'taman" degan eski yaxshi bahona yangi metodologiya tamoyillariga to'g'ri kelmaydi, shuning uchun u ba'zi qiyinchiliklarni keltirib chiqarishi mumkin.

4. Uydan Internetga kirish imkoni bo'lmagan talabalar uchun raqamli materiallardan foydalanish imkoniyatini ta'minlash. Variantlardan biri kerakli ma'lumotlarni disklarga yoki USB drayvlarga tashlashdir. Har holda, uyda o'z-o'zini o'rganish yangi metodologiyaning ajralmas elementidir.

5. Yangi ta'lim modelini tushuntirish uchun talabalarning ota-onalariga elektron pochta xabari yuborish; paydo bo'lgan savollarga javob berishga tayyor bo'ling. Innovatsion metodika o'qituvchining vazifasi sinfda materialni "chaynash" deb hisoblaydigan ko'plab ota-onalarga yoqmasa, hayron bo'lmang. Biroq, metodologiyani amalga oshirishning muvaffaqiyati ko'p jihatdan maktab o'quvchilarining ota-onalari uning samaradorligiga qanday ishonishlariga bog'liq bo'ladi.

Nima tavsiya etilmaydi:

1. Siz aytganingiz uchun talabalar materiallaringizni tomosha qilishlarini va/yoki o'qishlarini kutmang. Edmodo1 yordamida siz tegishli topshiriqlarni taqdimotlar bilan birga yuklab olishingiz va ularni darsdan oldin tekshirishingiz mumkin. Bundan tashqari, har bir dars boshida siz talabalarga oddiy interaktiv viktorinalar va mashqlarni taklif qilishingiz mumkin.

2. Agar uydan o'quv materiallaridan foydalanish imkoniga ega bo'lsa, barcha o'quvchilar darsda yaxshiroq ishlaydi deb o'ylamang. Mustaqil ta'lim

...taqdimning ko'payishi holida, vazifalarni qiyinchilik darajasi bo'yicha farqlash zarurati ortadi, chunki ba'zi talabalar ma'lumotlarning butun hajmini idrok etadilar, boshqalari esa bardosh bera olmaydi.

3. Hamkasblaringizdan yangi metodologiya tamoyillari bilan so'zsiz rozilik va ta'lim jarayonini qo'llab-quvvatlashni kutmang. Shu bilan birga, maktab talablariga javob beradigan baholash tizimi haqida o'ylash kerak. Qiyinchilik shundan iboratki, tavsiflangan tizim bo'yicha o'qiyotgan sinfdagi o'rtacha ko'rsatkich ko'pincha umumiy qabul qilingan ball shkalasining yuqori chegaralaridan tashqariga chiqadi.

4. Shuni unutmangki, yangi modelda ko'zda tutilgan sinfdagi mashg'ulotlar formati o'qituvchiga qo'yiladigan standart talablarga umuman javob bermaydi. Ochiq darsdan oldin, barcha kuzatuvchilarga materialni taqdim etish usuli haqida ma'lumot yuborishni unutmang. Shubhasiz, yangi tizim sizning malakangizni baholashga salbiy ta'sir ko'rsatishi mumkin bo'lgan darsda ma'lumotni kamroq hajmda taqdim etishni ta'minlaydi.

5. Siz ishlab chiqqan taqdimot materiali ko'p yillar davomida dolzarb bo'lib qoladi deb o'ylamang. Yangi metodika o'quvchilarning talab va istaklarini inobatga olgan holda axborot doimiy ravishda yangilanib tursagina samarali bo'ladi. Yaxshiyamki, iPad va shunga o'xshash qurilmalar ma'lumotlarni topish va taqdimotlar qilishni ancha osonlashtiradi.

**Nazorat savollari:**

1. Flipped Class haqida so'zlab bering?
2. Flipped ta'lim qanday g'oyalarga asoslanadi?
3. Adaptiv ta'lim tizimini izohlang.



# IV BOB. ELEKTRON ONLINE TA'LIMNING RIVOJLANISH TENDENSIYASI VA ISTIQBOLLARI

## 4.1. Elektron pedagogika va andragogikada o'quv motivatsiyasi omillari

**Reja:**

1. Kattalar ta'limi tashkil etishda elektron pedagogikaning ahamiyati
2. Androgogik model va uning asoslari
3. Nazariy va amaliy mashg'ulotlarni tashkil etishda elektron ta'lim resurslarining o'rni

**Kalit so'zlar:** Androgogik model, Distatsion usul, Ziyonet.

### *Kattalar ta'limi tashkil etishda elektron pedagogikaning ahamiyati*

"Andragogka" (yunoncha andros – katta inson, agoge – yo'l-yo'riq, tarbiya) atamasi birinchi marta 1833 yilda nemis o'qituvchisi K.Kapp tomonidan taklif qilingan. K.Kapp Platon (Aflotun)ning pedagogik qarashlarini o'rganar ekan, andragogika –pedagogikaning kattalar ta'limiga oid bo'limi deb ataydi.

Aflotunning "Davlat" dialogida ta'lim hokimiyat qo'lidagi kuchli qurol sifatida talqin qilinadi. Aflotun g'oyalarni bilishni inson faoliyatining oliy maqsadi deb hisoblagan va ta'lim bu jarayonga zarur tayyorgarlikni ta'minlashi kerak. Aflotun umumbashariy majburiy (kamida uch yillik) ta'lim tamoyilini e'lon qildi: "Keksalar ham, yoshlar ham o'z imkoniyatlari darajasida ta'lim olishlari kerak". Ammo qobiliyat ko'rsatganlar o'rganishni davom ettirishlari mumkin. Platon quyidagi o'qish davrlarini taklif qildi: 7 yilgacha - xalq ta'limi; 7 yoshdan 12 yoshgacha - davlat maktabi (o'qish, yozish, qo'shiq aytish, musiqa); 12 yoshdan 16 yoshgacha - "Palestra" - (jismoniy tarbiya); 16 yoshdan 18 yoshgacha - arifmetika, geometriya; 18 yoshdan 20 yoshgacha - harbiy tayyorgarlik; 21 yoshdan 31 yoshgacha - matematika, geometriya, astronomiya, musiqa; 31 yoshdan 35 yoshgacha - falsafa; 35 yoshdan boshlab odam jismoniy mashqlar bilan shug'ullanishi kerak.

Katta yoshdagi o'quvchilarning psixologik va fiziologik xususiyatlari

Ta'lim jarayoni doimo ta'lim sub'ektining fiziologik, psixologik, yosh va ijtimoiy o'ziga xos xususiyatlarini hisobga olgan holda quriladi.

Ko'p yillar davomida psixologlar an'anaviy ravishda psixikaning rivojlanishini faqat inson tanasining biologik rivojlanish davrlarida, ya'ni 15-17 yilgacha ko'rib chiqdilar. Psixikaning keyingi rivojlanishi kutilmadi. 18 yoshdan 60 yoshgacha bo'lgan davr "fosil" (E. Claparede) deb nomlangan. Inson hayotining ushbu segmenti statsionar holat, ya'ni hech qanday sifat yoki tarkibiy o'zgarishlarning yo'qligi bilan tavsiflanadi, deb ishonilgan. Psixofiziologiya, psixologiya va gerontologiyaning zamonaviy ma'lumotlari kattalarda psixikaning rivojlanishi davom etmoqda va bu jarayon bir nechta jarayonlarning kombinatsiyasida ifodalangan tarkibiy murakkablik bilan tavsiflanadi degan xulosaga kelishimizga imkon beradi:

Konstruktiv, funktsional darajaning oshishiga olib keladi;

Barqaror, funktsiyalarning barqarorligini tavsiflovchi;

Involyutsion, funktsiyalarning zaiflashishi va pasayishi bilan ifodalanadi.

Kattalar ta'limining ba'zi salbiy tomonlari ham bor, ular orasida quyidagilar mavjud:

- kasbiy qayta tayyorlash va malakasini oshirish, psixologlarning fikriga ko'ra, inson rivojlanishining eng qiyin bosqichlaridan biri - kasbiy faoliyatning ko'plab o'rnatilgan g'oyalari va stereotiplarini psixologik sindirish bilan bog'liq kasbiy qayta qurish bosqichi;

- o'quvchilarning yoshidagi sezilarli diapazon idrokning boshqa sifatini, xotiradagi farqlarni, o'rganish qobiliyatini keltirib chiqaradi, bu esa o'qituvchining o'quv maqsadlariga erishishini qiyinlashtiradi;

- talabalar kontingenti nazariy va kasbiy tayyorgarlik darajasi, ularning mehnat faoliyati xarakteri, ish tajribasi jihatidan xilma-xildir;

- ko'pincha talabalarning "psixologik inertsiyasi" bilan bog'liq muammolar mavjud stereotiplar, rad etish, uning qarashlari va tajribasiga zid bo'lgan narsalarni idrok etishni istamaslik.



Tarbiyachilar biladiki, ba'zi tushunchalarni kattalarga o'rgatish uchun ishlatiladigan usullar bolalarni o'qitish usullaridan tubdan farq qiladi. Bu tushuncha o'rnini andragogika va pedagogika deb nomlangan metodologiyalar egalladi. Katta yoshlilarga qaratilgan va ularni andragogika mavzusini yanada samarali va samarali o'rganishga qaratilgan strategiyalar. Garchi kontseptsiya 1833 yilda nemis o'qituvchisi Aleksandr Kapp tomonidan ilgari surilgan bo'lsa -da, u rasmiy ravishda AQShlik Malcolm Knowles tomonidan kattalar ta'limi mavzusiga aylandi.

Bu nazariyada kattalar ta'limining tayanchini tashkil etuvchi ba'zi asosiy taxminlar mavjud. Masalan, kattalar o'z ishi va shaxsiy hayotiga mos keladigan tushunchalarni o'rganishga ko'proq qiziqadi degan taxmin bor. Kattalar uchun tashqi motivatorlar emas, balki ichki motivatorlar kerak. Yangi tushunchalarni o'rganish tajribani talab qiladi, bu xatolarni ham o'z ichiga oladi. Kattalar o'z bahosini kuzatishda bolalarga qaraganda ko'proq mas'uliyatli bo'lishi mumkin.

Hamma narsani umumlashtirish uchun, Oksford lug'atida aytilganidek, andragogika - "Katta yoshdagi o'quvchilarni o'qitish usuli va amaliyoti; kattalar ta'limi. "

Hozirgi kunda ta'lim tizimiga berilayotgan katta e'tibor tizimning turli bosqichlariga alohida etibor qaratilishini va ushbu bosqichlarning o'ziga hos xususiyatlaridan kelib chiqqan xolda jarayonni tashkil etishni taqazo etmoqda. Ushbu nuqtai-nazardan, xalq ta'limi va oliy va undan keyingi ta'lim tizimi vakillari orasida ko'p muhokamaga sabab bo'luvchi pedagogika va andragogika tushunchasiga oydinlik kiritmoqchimiz.

So'zimizni boshini ko'pchiligimizga tanish bo'lgan pedagogika, ya'ni soha vakili bo'lgan "pedagog" tushunchasidan boshlamoqchimiz. Pedagog (Pedagogue), maktab o'qituvchisi – juda sinchkovlik yoki qat'iyatlik bilan ta'lim beruvchi kishi deb ta'riflanadi. Pedagogik modelda nimani, qachon va qanday o'qitilish kerakligini o'qituvchi hal qiladi.

Kattalarni o'qitish, o'rgatish sohasi hisoblangan "androgogika" esa, aksincha, kattalarga ta'lim beruvchi san'at va fan hisoblanadi. Androgogik model quyidagi beshta asosga tayanadi:

1) o'rganuvchilarga biror narsani o'rganish nima uchun muhimligi bildiriladi;

2) o'rganuvchilarga ma'lumotlar ichida o'zlarini qanday boshqarishni ko'rsatadi;

3) mavzu o'quvchilar tajribasiga bog'lanadi;

4) odamlar to o'rganishga tayyor bo'lmagunicha yoki motivlanmagunicha ishga kirishmaydilar;

5) Bu esa o'rganish bo'yicha to'siqlarni, xatti harakatlar va e'tiqodlarni bartaraf etishni talab qiladi.

Xulosa shuki, pedagogikadan farqli ravishda androgogikaning ta'limiy maqsadi o'rganuvchilarga mazmunni qabul qilishga va unga tanqidiy fikr bildirishga zamin yaratish hamda uni hayotda amaliy qo'llay olishda namoyon bo'ladi.

J.Rachal androgogikani kattalarga ta'lim berish vositasi sifatida o'rganib, oliy ta'limda talabalar o'z motivatsiyalariga o'zlari mas'ul bo'lishlari kerakligini ta'kidlaydi. Androgogika talabalarni nazorat qilishga, egallanayotgan bilimlarni mavjud standartlarga asoslanib baholab borishga va talabalarni o'rganishga ixtiyoriy jalb etishga chorlaydi. Lekin bu shartlarning aksariyati oliy ta'limda qo'llanmaydi.

Androgogikaning asosiy nazariyalaridan yana biri, o'qish / o'rganish haqiqiy qadriyat sifatida ta'qib qilinishidir. Androgogika qoniqishni ko'lamini va talaba belgilagan natija darajasini talab qiladi. Bu shartlarning hech birini oliy ta'lim mazmuni orasidan osonlikcha topib bo'lmaydi, ayniqsa, o'qitilishi nazarda tutilayotgan kursning maqsadiga qoniqish asosiy aniqlovchi sifatida kiritilmagan bo'lsa.

Bolalar ta'limida o'qituvchilar tashqi motivatsion omillar (baho olish, ota-onaning yoki o'qituvchining talabi, uyalib qolishdan qo'rqish va h.z.) sifatida muhim o'rinni egallasa, oliy ta'limda esa tashqi omillar o'quv faoliyati



samaradorligiga ta'sir ko'rsatsa-da, talaba mas'uliyatini kuchaytirmaydi. Bunday farqni ajrata bilgan oliy ta'lim o'qituvchisigina tegishli metod, texnologiya va yondashuv orqali talabalarga bilim olish ko'nikmalarini o'rgatishda muvaffaqiyatga erishadi.

Tadqiqotlar shuni ko'rsatadiki, muvaffaqiyatli o'qishga bo'lgan motivatsiya omili ko'pincha intellekt omilidan kuchliroqdir. O'rganish jarayonini yoqimli qilishda o'rganuvchilar motivatsiyasini qo'llab-quvvatlash muhimdir. Shu sababli motivatsiyani shakllantirish, rivojlantirish, kerakli darajada saqlashga doir metod hamda yondashuvlarni inobatga olib, darslar va o'quv materiallarini tashkillashtirgan holda olib borish talab etiladi.

Birinchidan, taqdim etilayotgan matnlar, audiovizual materiallar, vazifalar va dars mashg'ulotlari talabaning qiziqishlariga mos bo'lishi lozim.

Ikkinchidan, o'qituvchi talabalarga vazifalarni bajarilishini baholash imkonini berishi va ularning ehtiyojlari boshlang'ich rolni o'ynashi talab etiladi.

Uchinchi muhim narsa – mashg'ulotlardagi yumor, musiqa singari dars mavzusidan tashqari, qo'shimcha mashg'ulotlar komponentlari talabalarning o'qishga bo'lgan ishtiyoqini oshirish xususiyatlari hisoblanadi. Qo'shimcha mashg'ulotlar sifatida nafaqat yumor yoki ko'ngilochar mashg'ulotlar, balki talabalarning orasida kurs maqsadiga mos bellashuvlar uyushtirish, misol uchun, poster taqdimotlar, video taqdimotlar, loyiha ishlari, guruhlarda loyiha ishlarini tashkillashtirish va boshqalarni kiritishimiz mumkin.

Ta'lim taraqqiyotini tizmiy tasavvur qilish va undagi jarayonlarni modellashtirish, ta'lim sohasidagi eng maqbul(optimal) yo'lni tanlash, samarali usullami yaratish uchun yechim bo'lib hisoblanadi.

Modellashtirishning yo'lga qo'yilishi, zamonaviy information texnologiyalar nazariyasini yaratish hamda kompyuter tarmoqlari negizida ta'lim jarayonining barcha bo'g'inlarini uzluksiz axborot bilan ta'minlashni yo'lga qo'yadi, bugungi kunda zamonaviy axborot texnologiyalarining mavjud imkoniyatlaridan nafaqat ishlab chiqarishda, baiki ta'lim sohalarida ham keng foydalanilmokda:

-elektron pochta;

-o'zaro tarmoq orqali bog'lanish;

-internet tarmog'i.

Zamonaviy axborot texnologiyalaridan o'quv jarayonida samarali foydalanish quyidagi imkoniyatlarga yo'l ochib bermoqda:

-yuqori malakali kadrlar tayyorlash;

-zamonaviy axborot texnologiyalaridan foydalanishni o'rganish;

- zamonaviy axborot texnologiyalarining qo'shimcha qurilmalaridan foydalanishni o'rganish;

-dars jarayonlarini umumlashtirish va soddalashtirish;

-talabalarning darsga bo'lgan qiziqishlarini oshirish;

-talabalarni mustaqil fikrlashga, zamonaviy axborot texnologiyalari bilan ishlashga o 'rgatish va izlanuvchanligini oshirish.

Bu o'z navbatida hayotimizga yangi masofaviy ta'lim tizimini kirib kelishiga sabab bo'ldi. Masofaviy ta'lim qisman elektron darslik va kitoblardan iboratdir. Shuning uchun o'quv muassasalarining masofaviy ta'lim bo'limiga ega bo'lgan Web sahifalar yaratishi bugungi kunning dolzarb muammosidir.

Ushbu muammoni echish uchun O 'zbekiston Respublikasining Oliy va O'rta Maxsus Ta'lim vazirligi tomonidan masofaviy ta'lim tizimini yo'lga ko'yish bosqichlari belgilab qo'yilgan bo'lib, ushbu bosqichda ta'lim tizimiga masofaviy ta'limni joriy etish ko'zda tutiladi.

Kattalarni masofali o'qitishda Internet tarmog'ining o'rni.

Distatsion usuli asosida o 'qitishning o 'quv qoidalaridan kelib chiqsak, talabalar internet turi orqali jahon bo'yicha sayohat qilishlari mumkin. Shu bilan birga ta'lim berish uslubining o 'zgarishi bilan uning shakilari ham o'zgarishi shartdir. Hozirgi kunda to'g 'ridan -to'g 'ri Internet tarmog'iga kirish xizmati, distatstion uslubi asosida ta'iim berish uchun elektron pochtalar kompyuter konfirensiyalari va ma'lumotlaming elektron bazasida foydalaniladi.

Axborotlashgan tezkor kanalning rivojlanishi yangi gipermediya tizimini berib, u o'z ichida Internet tarmog'iga kirishning 3 ta asosiy qismini



mujassamlashtiradi va foydalanuvchining interfeysini (muloqoti) yanada takomillashtirishga yordam beradi. Masalan, maltikast texnologiyalarining konferensiya vositalarining va multimediya kompyuterlarining mavjudligi Internet tarmog'i orqali vidio konferensiyalami yo'lga qo'yishga imkoniyat berdi. Shunday qilib ligant axborotlashgan tarmoq, o'quvchilaming distant uslubi asosida zamonaviy bilim olishlari uchun vaqti yoki qaerda turganligiga qaramasdan keng sharoit yaratib beradi.

Infosfera nafaqat ishlab chiqarish, axborot ayirboshlash, iqtisodiy-ijtimoiy va ma'naviy-ma'rifiy sohalarda, baiki jahon ta'lim tizimini yangi bosqichga ko'tarishga va uni takomillashtirishga xizmat qilmoqda. Bu borada ta'lim sohasida masofali o 'qitish tizimining shakllanishi va uni yuqori malakali mutaxassislarni tayyorlashda xizmat qilishi muhim ahamiyat kasb etmoqda.

Hozirgi davrda, jahonning rivojlangan mamlakatlarida (AqSH, Buyuk Britaniya, YAponiya, Fransiya, Kanada, Rossiya, Italiya, Ukraina) masofali o'tish tizimining joriy etilishi natijasida umumjahon axborot resurslariga bo'lgan extiyoj keskin oshib borishi bilan bir qatorda, ularda maqsadli foydalanishning yangi usul hamda vositalari shakllandi.

Respublikamizda ham masofali o'tish tizimi joriy etish orasida dastlabki ijobiy ishlar amalga oshirildi. Jumladan, O'zbekiston respublikasi Prezidentining «Iste'dot» jamg'armasi qoshidagi «masofali o'qitish markazi» hamda Rossiyaning informastion jamiyatini rivojlantirish inistituti tomonidan masofali o'qitish kurslarining tashkil etilishi, Ushbu yo'nalish bo'yicha amalga oshirilgan ijobiy ishlarning daslabki de'bochasidir.

Albatta, masofali o'qitish tizimini joriy etish uchun bir qator tashkiliy, o'quv-uslubiy hamda iqtisodiy masalalami hal etishga to'g'ri keladi.

Fikrimizcha, bu vazifalarni ijobiy hal etish uchun respublikamizdagi bir qator oliy o'quv yurtlarining imkoniyatlari yetarlidir

Bugungi kunda taraqqiyot juda tez rivojlanmoqda va juda tez o'zgarmoqda. Deyarli har daqiqada sayyoramizning turli burchaklarida o'zgarishlar, yangiliklar va kutilmagan voqealar hodisalar sodir bo'lmoqda.

Har bir kunimiz informastiya oqimi ta'sirida kechmoqda. Ta'lim tizimida masofadan o 'qitish uslubi shakllari qo'llanilmoqda. Masofadan o 'qitish uslubi-bu sirtqi o'qishning yangi shaklidir. Masofadan o 'qitish bu mustaqil masofadan dars o'qishdir. Mustaqil o'qitish insonning mustaqil fikrlash, xolatni baholash, xulosa va bashorat qilish qobiliyatlarini shakllantiradi.

Masofali kurs shakli quyidagilardan tashkil topadi.

-kursning nomi

-o'qituvchining ism familyasi

-o'qituvchining elektron manzili

-kursga oid ma'lumotlar

-kurs materiallari

-talabalar

-yordam

sistemaga talablar:

tizim Windows va Internet Explorer 5.0 va undan yuqori turdagi programmalar doirasida ishlaydi. Tizim o'qituvchilar va talabalar uchun foydalanish ko'rsatmalariga ega. Dictatstion o'qitish tizimi O 'zbekiston Respublikasi Davlat Patent idorasida qayd etilgan.

Masofadan o'qitishning tarkibiy belgilari: o'qituvchi, o'quvchi, kommunikastiyadir.

Masofadan o 'qitishning uslubiy materiallari quyidagilardir:

Darslik

Audio va video darsliklar

On-layn darsiar (Internet saxifa)

Elektron kutubxonalar

Multimedia, elektron darsliklar

Masofadan o'qitishda virtual kutubxonalar sputnik orqali videokonferensiyalar, darsiar, Internet yordamida muloqot va informasiya olish imkoniyatlari paydo bo'ladi. Bu esa o 'quvchi uchun maxsus o'qish doirasini beradi.



*Nazariy va amaliy mashg'ulotlarni tashkil etishda elektron ta'lim resurslarining o'rni*

Ko'rinib turibdiki, amaliy mashg'ulotlarning asosiy tarbiyaviy maqsadi muayyan turdagi masalalarni yechish ko'nikma va malakalarini shakllantirishdan iborat. Shuning uchun bunday darsni o'tkazish jarayonida talabalarga taklif qilinadigan vazifalar soni nisbatan past darajadagi murakkablik bilan etarlicha katta bo'lishi kerak.

Hozirgi ta'lim tizimini axborotlashtirish davrida hosil bo'ladigan va qayta ishlanayotgan axborotlar hajmi kun sayin ortib, zamonaviy kompyuter va telekommunakasion texnologiyalari vositalari tez sur'atlar bilan mukammalashib va takomillashib borayotgan sharoitda ta'lim tizimini kerakli axborot manbalari bilan ta'minlash, ularni to'plash, saqlash va qayta ishlash usullari bo'yicha kerakli bilim va malakalarini shakllantirish muhim vazifalardan biri hisoblanadi. Shu bilan birga axborot texnologiyalarining zamonaviy vositalari ta'lim jarayonining barcha imkoniyatlari va tashkillashtirish usullarini butunlay o'zgartirib yuborish bilan birga, yangi pedagogik texnologiyalarining zamonaviy metodlarini, usullarini va dasturiy vositalarini tatbiq etish bo'yicha yanada kengroq imkoniyatlarni yaratib bermokda.

Bugungi kunda o'quv jarayonining barcha jabhalarida zamonaviy elektron axborot resurslarining, ko'plab axborot va kommunikasion texnologiya-larining, shu jumladan dasturiy jihozlash vositalarining keng imkoniyatlaridan foydalanish maqsadga muvofiqdir.

Dasturiy jihozlash vositalari – amaliy dasturiy jihozlar bo'lib, ular ta'lim tizimining barcha sohalarida dasturiy tizimlarni yaratish, tayyorlash, tashkiliy materiallarni va ma'lumotlarni jamlash, grafik yoki animasiyalarni qo'shish va namoyish uchun mo'ljallangan. Bunday vositalar yordamida o'quv jarayonini tashkil etish uchun multimedia kurslarini yaratish ko'proq samara beradi.

Multimedia kurslari asosida o'quv jarayonini tashkil etishda mash-g'ulot o'tishning turli uslublari va texnologiyalaridan foydalanish lozim bo'ladi. Buning uchun talabalarning o'quv auditoriyalarida, kompyuter sinf-larida, o'qitishning

texnik vositalari xonasida, uslubiy kabinetda amaliy shug'ullanishlarini tashkil etish lozim.

Bundan tashkari barcha multimedia o'quv kurslari amaliy tadbiqdan va tajribadan o'tgan bo'lishi bilan birga, o'ziga xos xususiyatlarga ham ega bo'lish bilan birga, ularning xususiyatlari bilim va ko'nikmalarni shakllantirish uchun foydalaniladigan o'quv materiallarining tasvirlanish formasiga va ko'rinishiga bog'liq bo'lishi kerak. Ular faqatgina misol va masalalar yechish, amaliy va laboratoriya mashg'ulotlarini bajarish jarayonidagina emas, balki butun o'quv jarayonida talabalarni professional bilim, malaka va ko'nikmalarini shakllantirishga qaratilishi lozim. Bu esa interfaol ma'ruzaviy multimedia kurslarini va namoyish materiallarini to'ldiruvchi, tradision usulda chop etishga asoslangan elektron o'quv qo'llanmalari yaratish lozimligini ko'rsatadi.

Interfaol multimediali kurslar turli xil axborotlarni – matn, statik va dinamik grafika, video va audio yozuvlarni integrasiyalash imkonini beradi . Ulardan foydalanish ma'ruzaviy namoyishlarning sifatli video yozuvlarini, kompyuterli laboratoriya ishlari va amaliyotlarni, hodisa va jarayonlarning imitasion animasiyali modellarini yaratish imkonini beradi, bu esa ro'y berayotgan jarayonlarni ta'sirchanligini va haqqoniyligini ko'rsata oladi xamda talabani o'quv jarayonida faolroq va diqqatliroq bo'lishga o'rgatadi.

Multimedia kurslarini yaratishda shu sohaning asosiy didaktik masalalaridan biri – o'qitishni modellashtirish va tasavvurlash obyektlariga ta'sir qilishning umumiy metodlari muhim o'rinlardan birini egallaydi.

Kompyuter yordamida modellashtirish turli jarayonlar va obyektlarni asosiy xossalarini tekshirish va namoyish qilish, u yoki bu nazariy ma'lumotlarni qo'llanilish holatini va chegarasini aniqlash imkonini beradi.

**Nazorat savollari**

1. Kattalar ta'limi tashkil etishda elektron pedagogikaning ahamiyati
2. Androgogik model nechta asosga tayanadi:



3. Kim androgogikani kattalarga ta'lim berish vositasi sifatida o'rganib, oliy ta'limda talabalar o'z motivatsiyalariga o'zlari mas'ul bo'lishlari kerakligini ta'kidlaydi?
4. Zamonaviy axborot texnologiyalaridan o'quv jarayonida samarali foydalanish qanday imkoniyatlarga yo'l ochib bermoqda?

## 4.2. Ta'lim portallari resurslari bilan ishlash

**Reja:**

1. Ta'limda portal texnologiyalari
2. Internet resurslaridan ta'lim jarayonida foydalanish
3. ZiyoNET Portali elektron kutubxonasining rivoji
4. ZiyoNET tarmog'i Resurs markazining asosiy vazifalari

### *Ta'limda portal texnologiyalari*

**Portal** (ing. **portal**; lotincha **porta** "darvoza"). Turli xil resurs va xizmatlardan tizimli tarzda ko'p pog'onali birlashma sifatida tashkil qilingan sayt. Foydalanuvchiga aniq axborot beradi, izlash tizimlari, elektron xaridlar, bepul elektron pochta, savdo reklamasi, xabarlarni birdaniga jo'natish, veb kimoshdi savdosi, chatlar kabi xizmatlardan bir onda foydalanish imkonini beradi. Portallar ko'plab foydalanuvchilarni jalb etish va ularning qiziqishlari haqida axborot yig'ish imkoniga ega. Ushbu atama umumiy turdagi, ya'ni Internetning ma'lum auditoriyasi uchun "boshlang'ich nuqta" rolini o'ynaydigan portallarga tegishlidir. Umumiy turdagi portallar gorizontal tashkiliy tuzilmaga ega bo'lib, bir necha mavzuni birlashtiradi.

**Ta'lim portali** – axborot-telekommunikatsiya tarmog'idan foydalangan holda foydalanuvchilarning keng doiradagi ta'lim axborot resurslari va xizmatlaridan foydalanishni ta'minlashga mo'ljallangan axborot tizimi. Ta'lim portallarida matnlar, interfaol darsliklar, virtual laboratoriyalar, videoroliklar va masofaviy ta'lim uchun ishlatilishi mumkin bo'lgan boshqa turdagi raqamli ta'lim

elementlariga XOR amali bilan qo‘shiladi. Masalan, dastlabki ochiq matn bloki quyidagicha bo‘lsin:

$$\begin{bmatrix} \{25\} & \{bd\} & \{b6\} & \{4c\} \\ \{d1\} & \{11\} & \{3a\} & \{4c\} \\ \{a9\} & \{d1\} & \{33\} & \{c0\} \\ \{ad\} & \{68\} & \{8e\} & \{b0\} \end{bmatrix}$$

Dastlabki raund kaliti esa quyidagiga teng bo‘lsin:

$$\begin{bmatrix} \{d4\} & \{7c\} & \{ca\} & \{11\} \\ \{d1\} & \{83\} & \{f2\} & \{f9\} \\ \{c6\} & \{9d\} & \{b8\} & \{15\} \\ \{f8\} & \{87\} & \{bc\} & \{bc\} \end{bmatrix}$$

U holda *AddRoundKey()* akslantirishining natijasi quyidagiga teng bo‘ladi:

$$\begin{bmatrix} \{25\} & \{bd\} & \{b6\} & \{4c\} \\ \{d1\} & \{11\} & \{3a\} & \{4c\} \\ \{a9\} & \{d1\} & \{33\} & \{c0\} \\ \{ad\} & \{68\} & \{8e\} & \{b0\} \end{bmatrix} \oplus \begin{bmatrix} \{d4\} & \{7c\} & \{ca\} & \{11\} \\ \{d1\} & \{83\} & \{f2\} & \{f9\} \\ \{c6\} & \{9d\} & \{b8\} & \{15\} \\ \{f8\} & \{87\} & \{bc\} & \{bc\} \end{bmatrix} =$$

$$\begin{bmatrix} \{25 \oplus d4\} & \{bd \oplus 7c\} & \{b6 \oplus ca\} & \{4c \oplus 11\} \\ \{d1 \oplus d1\} & \{11 \oplus 83\} & \{3a \oplus f2\} & \{4c \oplus f9\} \\ \{a9 \oplus c6\} & \{d1 \oplus 9d\} & \{33 \oplus b8\} & \{c0 \oplus 15\} \\ \{ad \oplus f8\} & \{68 \oplus 87\} & \{8e \oplus bc\} & \{b0 \oplus bc\} \end{bmatrix} =$$

$$\begin{bmatrix} \{f1\} & \{c1\} & \{7c\} & \{5d\} \\ \{00\} & \{92\} & \{c8\} & \{b5\} \\ \{6f\} & \{4c\} & \{8b\} & \{d5\} \\ \{55\} & \{ef\} & \{32\} & \{0c\} \end{bmatrix}$$

*Raund kalitlarini generatsiyalash.* AES shifrlash algoritmida raund kalitlari dastlabki kiritilgan shifrlash kalitidan hosil qilinib, u quyidagi jarayonlardan iborat:

- kalitni kengaytirish (Key Expansion);
- raund kalitlarini tanlash (Round Key Selection).



Raund kalitlarining umumiy bitlari soni kirish ma’lumotining bitlari sonini raund soniga ko‘paytmasiga va yana bitta kirish ma’lumotining bitlari sonini yig‘indisiga teng (misol uchun 128 bitli shifrlash uchun 128×10+128=1408 bit raund kaliti kerak bo‘ladi), ya’ni $N_b\,(N_r + 1) = 128 \times (10 + 1) = 128 \times 11 = 1408$ bit.

Demak, 128 bit uzunlikdagi blok va 10 raund uchun 1408 bit raund kalitlari talab qilinadi. 128 bitli kalit uzunligi uchun raund kalitlarini generatsiyalash jarayonini ko‘rib o‘taylik.

Dastlabki kalitni kengaytirishda, dastlab 128 bitli (16 bayt) boshlang‘ich kiruvchi kalit kiritiladi va to‘rtta ($w_0$, $w_1$, $w_2$, $w_3$) 32 bitdan bo‘lgan bo‘lakka bo‘linadi. Qolgan kengaytirilgan kalitlar mana shu to‘rtta ($w_0$, $w_1$, $w_2$, $w_3$) kalitlar yordamida topiladi. Ya’ni, kengaytirilgan kalitlar quyida keltirilgan (5.2) va (5.3) formulalar asosida hisoblab topiladi. Kengaytirilgan kalitlar soni $N[w(i)] = N_b(N_r + 1)$ tenglik bilan hisoblanadi. Xususan, 128 bitli kalit uchun $N_b = 4, N_r = 10$ ga tengligi bois, $N[w(i)] = 4(10 + 1) = 44$ ga teng.

Demak, 128 bitli kirish blokiga va 10 ta raundga ega bo‘lgan shifrlash uchun 44 ta kengaytirilgan kalitlar kerak bo‘ladi.

Raund kalitlari kengaytirilgan kalitlardan quyida bayon qilingan qoida asosida yaratiladi. Kalitlar generatsiyasining formulalari quyidagi ko‘rinishga ega:

$$w[i] = w[i-1] \oplus w[i - N_k], \tag{5.2}$$

va

$$w[i] = SubWord(RotWord(w[i-1])) \oplus Rcon[i/N_k] \oplus w[i - N_k] \tag{5.3}$$

128 bitli kalit uchun raund kalitlarini generatsiyalashga oid misol 1-ilovaga keltirilgan.

## 5.4. ГОСТ 28147-89 simmetrik blokli shifrlash standarti

ГОСТ 28147-89 kriptoalgoritmi hozirda Rossiya Federatsiyasi davlat standart shifrlash algoritmi hisoblanadi. Bu algoritm apparat va dasturiy ta’minot uchun mo‘ljallangan bo‘lib, himoyalanadigan ma’lumotning maxfiylik darajasiga chegara yo‘q. Algoritmning kalit uzunligi 256 bitga shifrlashni 64 bit uzunlikdagi bloklarda amalga

oshiradi va raundlar soni 32 ga teng. Ushbu algoritm Feystel tarmog'iga asoslangan bo'lib, asosiy shifrlash rejimi oddiy almashtirishga asoslangan (bundan tashqari, murakkablikka asoslangan gammalishtirish rejimi, qayta aloqali gammalashtirish rejimi va xesh funksiya sifatida foydalanishga mo'ljallangan imitoqo'yish rejimi mavjud).

ГОСТ 28147-89 shifrlash algoritmining matematik asosi quyidagi amallarga asoslanadi:

- $mod2^{32}$ bo'yicha qo'shish amali. Ushbu jarayonda ma'lumot blokining o'ng qismi va 32 bitli raund kaliti $mod2^{32}$ amali asosida qo'shiladi. Ushbu amal XOR amaliga qaraganda kriptobardoshli sanaladi.
- Almashtirish jadvali orqali o'rin almashtirish. Ushbu amal ГОСТ 28147-89 algoritmida foydalanilgan yagona chiziqsiz funksiya bo'lib, u maxfiylik darajasini yanada oshiradi.
- Siklik surish amali. Ushbu amal chiziqli funksiya hisoblanadi. 32 bitli ma'lumotni 11 bit siklik chapga surish orqali amalga oshiriladi.
- XOR amalida qo'shish. Ushbu amalda ma'lumotning chap tomoni va 11 bit siklik surilgan o'ng tomon qo'shiladi.

Ushbu kriptografik algoritm o'zida yuqorida ko'rsatilgan sodda matematik amallarni birlashtirgan bo'lib, bu imkoniyat shifrlash/ rasshifrovkalashda katta tezlikni beradi.

*ГОСТ 28147-89 algoritmida kalit generatori.* Kiritilgan 256 bitli $K$ kalit 32 bitli 8 ta teng qismlarga ajratiladi: $K = K_0K_1K_2K_3K_4K_5K_6K_7$. Shundan so'ng, ushbu qismkalitlarni quyidagicha foydalanish orqali 32 raund uchun raund kalitlari shakllantiriladi:

| Raundlar soni | Kalitlar |
|---|---|
| 1-8 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 9-16 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 17-24 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 25-32 | $K_7K_6K_5K_4K_3K_2K_1K_0$ |

Biror ma'lumotni ГОСТ 28147-89 kriptoalgoritmi bilan shifrlash uchun dastlab 256 bitli kalitdan 32 ta 32 bitli rund kalitlari $K_i$ generatsiya qilinadi va ochiq ma'lumot 64 bitli $X_i$, $i = 1,2,...$ bloklarga



bo'linadi. Bu 64 bitli $X_i$ blok 32 bitli chap $L_i$ va o'ng $R_i$ qismlarga bo'linadi $X_i = L_i \| R_i$ va $\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}$ formula yordamida almashtiriladi, ya'ni shifrlanadi.

Kriptoalgoritmning $F$ funksiyasi quyidagi amal va almashtirishlardan tashkil topgan:

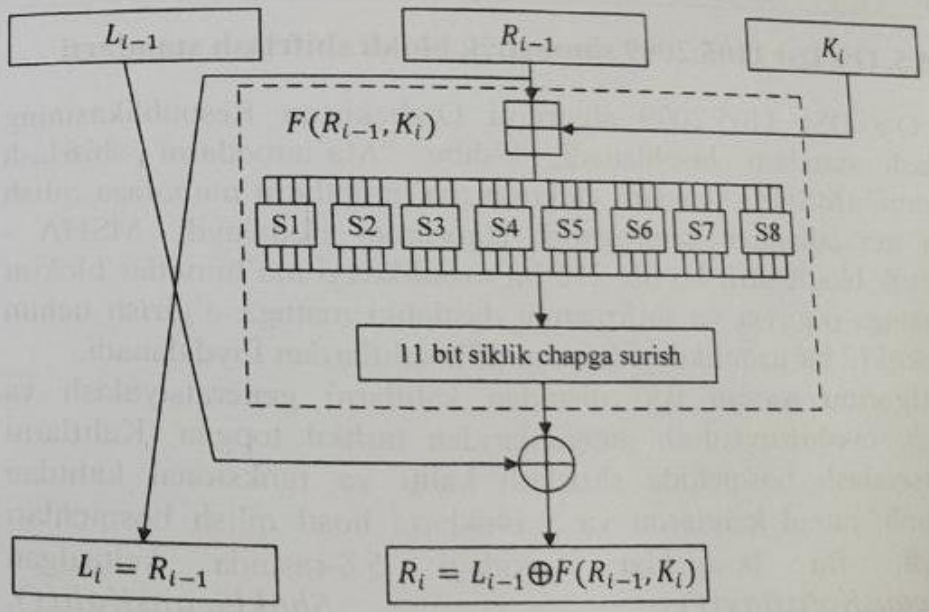
1)Blokning 32 bitli o'ng qismi va 32 bitli raund kalitini $mod2^{32}$ bo'yicha qo'shish: $C_i = (R_{i-1} + K_i) mod 2^{32}$;

2) 32 bitli $C_i$ natija sakkizta maxfiy S-bloklarda o'rniga qo'yish akslantirishi orqali akslanadi ;

3)S-bloklarda chiquvchi 32 bitli blok chapga 11 birlik siklik suriladi;

4)Ochiq ma'lumot 32 raund iterativ shifrlashdan so'ng, chap $L_{32}$ va o'ng $R_{32}$ qismlar birlashtiriladi va $Y_i = R_{32} \| L_{32}$ shifrma'lumot, ya'ni $Y_i$ shifrma'lumot hosil qilinadi.

ГОСТ 28147-89 kriptoalgoritmining $i$-raundining funksional sxemasi quyida keltirilgan:




*5.7-rasm.* **ГОСТ 28147-89 kriptoalgoritmining $i$-raundi**

Ushbu algoritm to'rt xil rejimda ishlaydi:

- oddiy almashtirish;
- gammalashga asoslangan;
- teskari aloqali gammalashga asoslangan;
- imitoqo'yish rejimi.

ГОСТ 28147-89 kriptoalgoritmida foydalanilgan S-bloklar statik emas. Turli tashkilotlar tomonidan turli S-bloklardan foydalanilgan. Quyida Rosstandartning "Axborotning kriptografiya himoyasi" bo'yicha standartida keltirilgan S-blok keltirilgan.

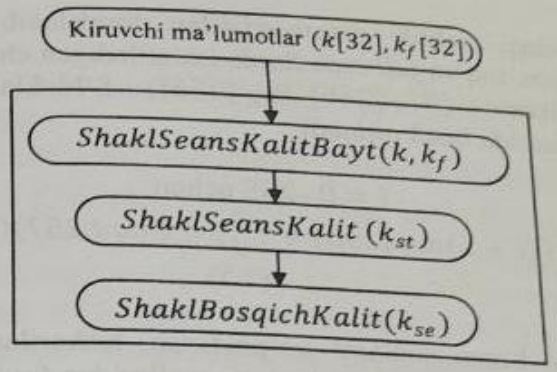
| S-blok raqami | Qiymatlari | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| 1 | C | 4 | 6 | 2 | A | 5 | B | 9 | E | 8 | D | 7 | 0 | 3 | F | 1 |
| 2 | 6 | 8 | 2 | 3 | 9 | A | 5 | C | 1 | E | 4 | 7 | B | D | 0 | F |
| 3 | B | 3 | 5 | 8 | 2 | F | A | D | E | 1 | 7 | 4 | C | 9 | 6 | 0 |
| 4 | C | 8 | 2 | 1 | D | 4 | F | 6 | 7 | 0 | A | 5 | 3 | E | 9 | B |
| 5 | 7 | F | 5 | A | 8 | 1 | 6 | D | 0 | 9 | 3 | E | B | 4 | 2 | C |
| 6 | 5 | D | F | 6 | 9 | 2 | C | A | B | 7 | 8 | 1 | 4 | 3 | E | 0 |
| 7 | 8 | E | 2 | 5 | 6 | 9 | 1 | C | F | 4 | B | 0 | D | A | 3 | 7 |
| 8 | 1 | 7 | E | D | 0 | 5 | 8 | 3 | 4 | F | A | 6 | 9 | C | B | 2 |

### 5.5. O'z Dst 1105:2009 simmetrik blokli shifrlash standarti

O'z DSt 1105:2009 algoritmi O'zbekiston Respublikasining shifrlash standarti hisoblanadi. Ushbu "Ma'lumotlarni shifrlash algoritmi" (MSHA) standarti elektron ma'lumotlarni muhofaza qilish uchun mo'ljallangan kriptografik algoritmni ifodalaydi. MSHA - simmetrik blokli shifr bo'lib, 256 bit uzunlikdagi ma'lumotlar blokini shifrmatnga o'girish va shifrmatnni dastlabki matnga o'girish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitlardan foydalanadi.

Algoritm asosan ikki qismdan kalitlarni generatsiyalash va shifrlash/ rasshifrovkalash jarayonlaridan tashkil topgan. Kalitlarni generatsiyalash bosqichida shifrlash kaliti va funksional kalitdan foydalanib, raund kalitlarini va $S$ bloklarni hosil qilish bosqichlari bajariladi. Bu bosqichlar quyidagi 5.8-rasmda keltirilgan $ShaklSeansKalitBayt()$, $ShaklSeansKalit()$, $ShaklBosqichKalit()$ funksiyalarini ketma-ket bajarish orqali amalga oshiriladi.






*5.8-rasm.* **Raund kalitlari va $S$ bloklarni generatsiyalash tartibi**

$$ShaklSeansKalitBayt(k[32], k_f[32]$$

almashtirish funksiyasining vazifasi seans kalitini hosil qilish va uning yordamida $S$ bloklarni generatsiyalashdan iborat.

Seans kaliti

$$k_{se} = k + k' * (1 + k_f * k) \qquad (5.4)$$

formula yordamida hosil qilingan qiymatning chapdan *672* bitini ajratib olish orqali hosil qilinadi.

Bu yerda, $k$ va $k_f$ - mos holda tanlangan shifrlash va funksional kalitlar, $k' - k_f$ ning o'ngdan *192* bitli qismi hisoblanadi.

Hosil qilingan seans kaliti yordamida $S-$ bloklarni generatsiyalash quyidagi tartibda amalga oshiriladi:

– $k_{se}$ seans kalitining o'ngdan *256+64* bitli qismi ajratib olinadi va uning chapdan *256* bitli qismidan baytli elementlardan tarkib topgan chiziqli massiv $k_{st} = [0,1,2,3, \ldots 31]$, qolgan *64* bitli qismidan – bayt sathida elementlardan tarkib topgan chiziqli massiv $B = [0,1,2,3,4,5,6,7]$ shakllantiriladi;

– chiziqli massiv $B$ elementlari $B_1 = [0,1,2,3]$ va $B_2 = [4,5,6,7]$ massivlarga ajratiladi va ulardan ma'lum qoidalar asosida $(d_1, R_1, L_1)$ va $(d_2, R_2, L_2)$ parametrlar uchliklari shakllantiriladi.

Yuqoridagi uchlik parametrlardan foydalanib bayt sathida shifrlash uchun, toq va juft raundlarda ishlatiladigan chiziqli massivlar juftligidan iborat $(B_{1A}[256], B_{2A}[256])$ S-bloklar quyidagicha formula yordamida hosil qilinadi:

$$i = 0 \div 255 \text{ uchun}$$
$$b_{sA}[i] \equiv \Big(\big((i+L) mod 256\big) + 1\Big)^{\backslash ds} (mod\ 257)(mod\ 256) \quad (5.5)$$

bu yerda, butun sonlarni ko'paytirish, teskarilash va darajaga oshirish deb atalgan parametrli algebra amallaridan foydalaniladi.

$X$ ni $Y$ ga $p$ modul bo'yicha $R$ parametrli ko'paytirish quyidagicha bajariladi:

$$X \circledR Y (mod\ p) \equiv X + Y(1 + RX)(mod\ p) \quad (5.6)$$

$X$ o'zgaruvchini $p$ modul bo'yicha $R$ parametrli teskarilash quyidagicha bajariladi:

$$X^{\backslash -1} (mod\ p) \equiv -X(1 + RX)^{-1} (mod\ p) \quad (5.7)$$

bu yerda $X^{\backslash -1} \circledR X \equiv 0\ (mod p)$, 0 – parametrli gruppaning birlik asosidir.

*Misol.* $X$ ni $p$ modul bo'yicha $R$ parametr $d$ darajaga oshirish amali $X^{\backslash d}(mod p)$ ko'rinishida ifodalanadi:

Masalan $X = 3$, $R = 7$, $d = 35$, $p = 256$ bo'lganda $X^{\backslash 35}$ kuyidagicha hisoblanadi:

$$X^{\backslash 35} \equiv X^{\backslash 32+2+1} \equiv \left(\left(\left(X^{\backslash 2}\right)^{\backslash 2}\right)^{\backslash 2}\right)^{\backslash 2} \circledR X^{\backslash 2} \circledR X (mod\ p)$$

bu yerda: $X^{\backslash 2}(mod\ p) \equiv X(2 + XR)(mod\ p)$

Qiymatlarni o'rniga qo'yib quyidagiga ega bo'linadi:

$$X^{\backslash 2}(mod\ p) \equiv 3(2 + 3 * 7)(mod\ 256) = 69$$



$$\begin{aligned} X^{\backslash 35} &\equiv (((69)^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR 3^{\backslash 2} \circledR 3 (mod\ 256) \\ &\equiv (69 \\ &\quad * (2 + 69 * 7) mod 256)^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR 3^{\backslash 2} \circledR 3 (mod\ 256) \\ &\equiv ((185 \\ &\quad * (2 + 185 * 7)(mod\ 256))^{\backslash 2})^{\backslash 2} \circledR 3^{\backslash 2} \circledR 3 (mod\ 256) \\ &\equiv \left(73 * (2 + 73 * 7)(mod\ 256)\right)^{\backslash 2} \circledR 3^{\backslash 2} \circledR 3 (mod\ 256) \\ &\equiv 73 * (2 + 73 * 7)(mod\ 256) \circledR 3^{\backslash 2} \circledR 3 (mod\ 256) \\ &\equiv 73 \circledR 69 \circledR 3 \equiv (73 + 69 * (1 + 7 * 73))(mod\ 256) \circledR 3 \\ &\equiv 73 \circledR 3 \equiv \big(73 + 3 * (1 + 7 * 73)\big)(mod\ 256) \equiv 73 \end{aligned}$$

Keyingi qadamda $ShaklSeansKalit$ $(k_{st})$ funksiyasi yordamida shifrlash va rasshifrovkalashda ishlatiladigan diamatritsalar quyidagicha generatsiya qilinadi:

– baytli elementlardan tarkib topgan chiziqli massiv $k_{st} =$ [0,1,2,3, ... 31] ning chapdan *20* baytli elementlaridan tarkib topgan chiziqli massiv qismi $K_{ss} = [0,1,2,3, \dots 19]$ ajratib olinadi;

– $i = 0 -- 19$ uchun, agar $K_{ss}[i] = 0$ bo'lsa, u holda $K_{ss}[i]$ ni $K_{ss}[i] - 1 (mod\ p)$ ga almashtiriladi.

Chiziqli massiv $K_{ss}$ ning elementlaridan ikki o'lchamli $K_1[4,4]$ va $K_2[4,4]$ massivlari quyidagi tartibda shakllantiriladi:

chiziqli massiv $K_S = [0,1,2,3, \dots 19]$ ikkita chiziqli massivlar $k_{s1} = [0,1,2,3, \dots 9]$ va $k_{s2} = [10,11,12,13 \dots, 19]$ ga ajratiladi va ularning har biri mos tarzda tartiblangan to'plam $\{k_{s1}[0,1], k_{s1}[0,2], k_{s1}[0,3], k_{s1}[1,0], \{k_{s1}[2,0], k_{s1}[2,1], k_{s1}[2,2], k_{s1}[3,0], k_{s1}[3,1], k_{s1}[3,2]\}$ va $\{k_{s2}[0,1], k_{s2}[0,2], k_{s2}[0,3], k_{s2}[1,0], k_{s2}[2,0], k_{s2}[2,1], k_{s2}[2,2], k_{s2}[3,0], k_{s2}[3,1], k_{s2}[3,2]\}$ ga o'zaro – bir qiymatli akslantiriladi va ularning har biridan mos tarzda ikkita $K_1[4,4]$ va $K_2[4,4]$ massivlarining $k_1[i,j]$, $k_2[i,j]$ elementlari shakllantiriladi (bu yerda, $i, j \in \{0,1,2,3\}$).

$K_S[4,4], s \in \{1,2\}$ massivlarining qolgan elementlari quyidagi qoida asosida shakllantiriladi:

– $j \in \{0,1,2,3\}$ uchun $i = j$ bo'lganda, elementlar aynan va qiymati bo'yicha $K_s[2,2]$ elementga teng;

– $i = 1, j = 0,2,3$ uchun elementlar aynan va qiymati bo'yicha $K_s[1,0]$ elementga teng;

– $i = 2, j = 0,3$ uchun elementlar aynan va qiymati bo'yicha $K_s[2,0]$ elementga teng.

Natijada, *sh*-shifrlash rejimida foydalanish uchun $K_s[8,4]$ sifatida quyidagi $K_1[4,4]$ va $K_2[4,4]$ ikkita maxsus tuzilmali diamatritsa shakllanadi.

Massiv $K_1$

| | | | |
|---|---|---|---|
| $k_1$ [0,0] | $k_1$ [0,1] | $k_1$ [0,2] | $k_1$ [0,3] |
| $k_1$ [1,0] | $k_1$ [1,1] | $k_1$ [1,2] | $k_1$ [1,3] |
| $k_1$ [2,0] | $k_1$ [2,1] | $k_1$ [2,2] | $k_1$ [2,3] |
| $k_1$[3,0] | $k_1$ [3,1] | $k_1$ [3,2] | $k_1$ [3,3] |

Massiv $K_2$

| | | | |
|---|---|---|---|
| $k_2$ [0,0] | $k_2$ [0,1] | $k_2$ [0,2] | $k_2$ [0,3] |
| $k_2$ [1,0] | $k_2$ [1,1] | $k_2$ [1,2] | $k_2$ [1,3] |
| $k_2$ [2,0] | $k_2$ [2,1] | $k_2$ [2,2] | $k_2$ [2,3] |
| $k_2$[3,0] | $k_2$ [3,1] | $k_2$ [3,2] | $k_2$ [3,3] |

*sh* - shifrlash rejimidan foydalanishda maxsus tuzilmali diamatritsa $K_1[4,4]$ uchun teskari maxsus tuzilmali diamatritsa $K_{1t}[4,4]$ hisoblanadi. Shuningdek, *dsh* - rasshifrovkalash rejimidan foydalanishda ham maxsus tuzilmali diamatritsa $K_2[4,4]$ uchun teskari maxsus tuzilmali diamatritsa $K_{2t}[4,4]$ hisoblanadi.

Diaaniqlovchisi noldan farqli maxsus tuzilmali diamatritsa $K_{1t}[4,4]$ ni (bu yerda, $i = \{1,2\}$) teskarilash uning ustida diaalmashtirish natijasida hosil bo‘lgan matritsaning teskari matritsasini hisoblash va hosil bo‘lgan teskari matritsa ustida diaalmashtirish amalini bajarish natijasini olishdan iborat.

Teskarilash natijasida ikkala $K_{1t}[4,4]$ va $K_{2t}[4,4]$ ham maxsus tuzilmali diamatritsa ko‘rinishiga ega bo‘lgan quyidagi $K_{1t}$ va $K_{2t}$ massivlar hosil bo‘ladi:



Massiv $K_{1t}$

| | | | |
|---|---|---|---|
| $k_{1t}$ [0,0] | $k_{1t}$[0,1] | $k_{1t}$[0,2] | $k_{1t}$ [0,3] |
| $k_{1t}$ [1,0] | $k_{1t}$[1,1] | $k_{1t}$[1,2] | $k_{1t}$ [1,3] |
| $k_{1t}$ [2,0] | $k_{1t}$[2,1] | $k_{1t}$[2,2] | $k_{1t}$ [2,3] |
| $k_{1t}$[3,0] | $k_{1t}$[3,1] | $k_{1t}$[3,2] | $k_{1t}$ [3,3] |

Massiv $K_{2t}$

| | | | |
|---|---|---|---|
| $k_{2t}$ [0,0] | $k_{2t}$ [0,1] | $k_{2t}$ [0,2] | $k_{2t}$ [0,3] |
| $k_{2t}$ [1,0] | $k_{2t}$ [1,1] | $k_{2t}$ [1,2] | $k_{2t}$ [1,3] |
| $k_{2t}$ [2,0] | $k_{2t}$ [2,1] | $k_{2t}$ [2,2] | $k_{2t}$ [2,3] |
| $k_{2t}$[3,0] | $k_{2t}$ [3,1] | $k_{2t}$ [3,2] | $k_{2t}$ [3,3] |

*sh*-shifrlash rejimidan foydalanishda $(K_{1t}, K_2)$ juftlik, *dsh*-rejimidan foydalanishda esa $(K_1, K_{2t})$ juftlik ishlatiladi.

Keyingi bosqichda $ShaklBosqichKalit(k_{se})$ almashtirish funksiyasi (chiziqli seans-bosqich kaliti massivini shakllantirish) yordamida raund kalitlari quyidagicha generatsiya qilinadi:

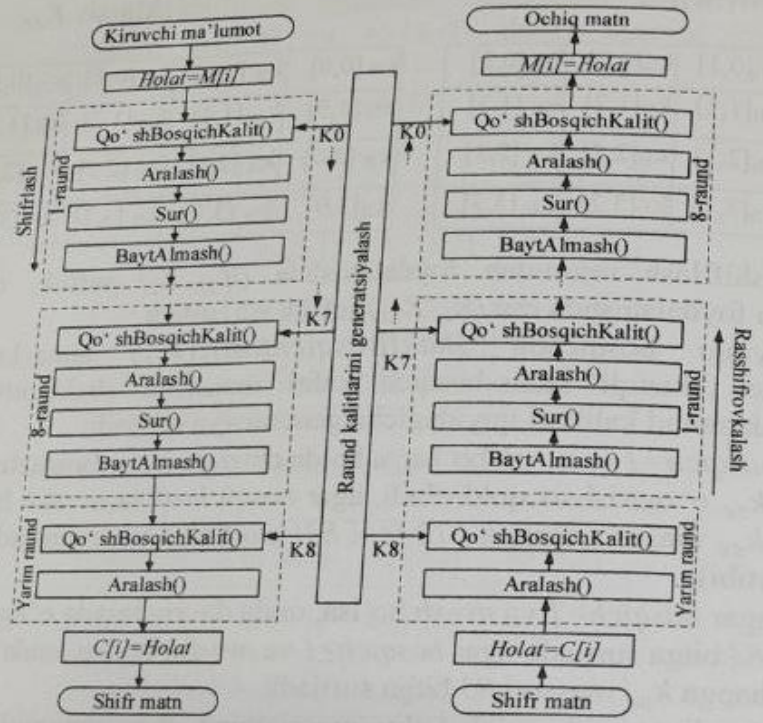
– *bosqich=1* va *m=sh* bo‘lsa, u holda chiziqli seans-bosqich kaliti massivi $k_{se}$ o‘zgarishsiz qoldiriladi, agar *bosqich=0* va *m=dsh* bo‘lsa, u holda $k_{se}$ massivi o‘ngga $672\text{-}(e \times 83) \bmod 672$ bitga suriladi ($e$ – raund tartibi);

– agar *bosqich>1* va *m=sh* bo‘lsa, unda davriy tarzda o‘ngga $k_{se}$ massivi *83* bitga suriladi, agar *bosqich≥1* va *m=dsh* bo‘lsa, unda davriy tarzda chapga $k_{se}$ massivi *83* bitga suriladi.

Chiziqli seans-bosqich kaliti massivining chap tomonidan *256* bitli qismini ajratib olib, undan elementlari bayt sathida berilgan $K_e[8,4]$ massivi shakllantiriladi. Bu almashtirish shifrlash jarayoni boshlangunga qadar hamma bosqichlar uchun amalga oshiriladi.

*S* bloklar generatsiya qilingandan so‘ng shifrlash va rasshifrovkalash jarayoni quyidagi 5.9-rasmda ko‘rsatilgan sxema asosida bajariladi.

Dastlab matnni shifrmatnga almashtirish rejimida ochiqmatn, shifrmatnni dastlabki matnga almashtirish rejimida esa shifrmatn kriptografik modulning *Holat[8,4]* massiviga yuklanadi. Keyin 8 ta raundning har birida *Qo'shBosqishKalit (Holat, $K_e$)*, *Aralash(Holat, $K_s$)*, *Sur(Holat)*, *BaytAlmash(Holat,$B_a$)* funksiyalari bajariladi. 8-raund tugagandan so‘ng esa faqat *Qo'shBosqichKalit (Holat, $K_e$)*, *Aralash (Holat, $K_s$)* funksiyalari bajariladi. Shifrlash jarayoni 2 xil rejimda amalga oshiriladi. Bular shifrmatn bloklarini ilaktirish (Cipher block chaining, CBC) va elektron kod kitobi (Electronic code book, ECB) rejimlaridir.




*5.9-rasm.* **Elektron kod kitobi rejimida shifrlash va rasshifrovkalash jarayoni blok sxemasi**

Ochiqmatn *Holat[8,4]* massiviga yuklangandan so'ng *Qo'shBosqichKalit(Holat, $K_e$)* funksiyasi yordamida *Holat* massivi va $K_e[8,4]$ seans kaliti massivlarining har bir bayt sathidagi bir nomli elementlari ustida XOR amali quyidagi tartibda bajariladi:

$0 \le c < 8$ uchun

$$[h'[c,0], h'[c,1], h'[c,2], h'[c,3]] = [h[c,0], h[c,1], h[c,2], h[c,3]] \oplus [ke[c,0], ke[c,1], ke[c,2], ke[c,3]].$$

Natija *Holat* massiviga ko'chiriladi. Keyin *Sur (Holat)* funksiyasi bajariladi. *Sur (Holat)* almashtirishi agar $m=$ *sh* rejimida bo'lsa, unda davriy tarzda *Holat* massivining $j$ −ustuni avvalo, pastga $(j+1)\ (mod\ 8)$ baytga suriladi, keyin hosil bo'lgan massivning $i$ −satri



o'ngga $(i+1)\ (mod\ 4)$ baytga suriladi, aks holda $m=dsh$ bo'lsa, unda davriy tarzda *Holat* massivining $i$ −satri avvalo, chapga $(i+1)\ (mod\ 4)$ baytga suriladi, so'ngra hosil bo'lgan massivning j-ustuni yuqoriga $(j+1)\ (mod\ 8)$ baytga suriladi. Bu yerda, $0 \le i < 4, 0 \le j < 8$.

Keyingi amal *Aralash (Holat, $K_s$)* quyidagi amallarni bajarishdan iborat:

– agar $m=sh$ bo'lsa, unda $K_1 = K_{1t}$, $K_2 = K_2$ qabul qilinadi, $H_1 \circledR_2 K_1 (mod\ p), H_2 \circledR_2 K_2\ (mod\ p)$ hisoblanadi, natija $H_1, H_2$ massivlariga yozilib, *Holat* massiviga ko'chiriladi, aks holda, ya'ni $m=dsh$ bo'lsa, unda $K_1 = K_1$, $K_2 = K_{2t}$ qabul qilinadi, $H_1 \circledR_2 K_1 (mod\ p), H_2 \circledR_2 K_2\ (mod\ p)$ hisoblanadi, natija $H_1, H_2$ massivlariga yozilib, *Holat* massiviga ko'chiriladi. $H_1 \circledR_2 K_1 (mod\ p), H_2 \circledR_2 K_2\ (mod\ p)$ ochiq matn biti $H_i\, i \in [1,2]$ ni maxsus tuzilmali diamatritsaga ko'paytirish qo'yidagi qoidalar asosida amalga oshiriladi:

| | |
|---|---|
| *h'[0,0]* | $h'_0 = h_0(k_0+k_4+k_8+k_{12}) + h_5k_4 + h_{10}k_8 + h_{15}k_{12} (modp)$ |
| *h'[1,1]* | $h'_5 = h_5(k_1+k_5+k_9+k_{13}) + h_0k_1 + h_{10}k_9 + h_{15}k_{13} (modp)$ |
| *h'[2,2]* | $h'_{10} = h_{10}(k_2+k_6+k_{10}+k_{14}) + h_0k_2 + h_5k_6 + h_{15}k_{14} (modp)$ |
| *h'[3,3]* | $h'_{15} = h_{15}(k_3+k_7+k_{11}+k_{15}) + h_0k_3 + h_5k_7 + h_{10}k_{11} (modp)$ |
| *h'[0,1]* | $h'_1 = h_1(k_1+k_5+k_9+k_{13}) + (h_0+h_4+h_8+h_{12})k_1 + h_2k_9 + h_3k_{13} (modp)$ |
| *h'[0,2]* | $h'_2 = h_2(k_2+k_6+k_{10}+k_{14}) + (h_0+h_4+h_8+h_{12})k_2 + h_1k_6 + h_3k_{14} (modp)$ |
| *h'[0,3]* | $h'_3 = h_3(k_3+k_7+k_{11}+k_{15}) + (h_0+h_4+h_8+h_{12})k_3 + h_1k_7 + h_2k_{11} (modp)$ |
| *h'[1,0]* | $h'_4 = h_4(k_0+k_4+k_8+k_{12}) + (h_1+h_5+h_9+h_{13})k_4 + h_0k_8 + h_7k_{12} (modp)$ |
| *h'[1,2]* | $h'_6 = h_6(k_2+k_6+k_{10}+k_{14}) + (h_1+h_5+h_9+h_{13})k_6 + h_4k_2 + h_7k_{14} (modp)$ |
| *h'[1,3]* | $h'_7 = h_7(k_3+k_7+k_{11}+k_{15}) + (h_1+h_5+h_9+h_{13})k_7 + h_4k_3 + h_6k_{11} (modp)$ |
| *h'[2,0]* | $h'_8 = h_8(k_0+k_4+k_8+k_{12}) + (h_2+h_6+h_{10}+h_{14})k_8 + h_9k_4 + h_{11}k_{12} (modp)$ |
| *h'[2,1]* | $h'_9 = h_9(k_1+k_5+k_9+k_{13}) + (h_2+h_6+h_{10}+h_{14})k_9 + h_8k_1 + h_{11}k_{13} (modp)$ |
| *h'[2,3]* | $h'_{11} = h_{11}(k_3+k_7+k_{11}+k_{15}) + (h_2+h_6+h_{10}+h_{14})k_{11} + h_8k_3 + h_9k_7 (modp)$ |
| *h'[3,0]* | $h'_{12} = h_{12}(k_0+k_4+k_8+k_{12}) + (h_3+h_7+h_{11}+h_{15})k_{12} + h_{13}k_4 + h_{14}k_8 (modp)$ |
| *h'[3,1]* | $h'_{13} = h_{13}(k_1+k_5+k_9+k_{13}) + (h_3+h_7+h_{11}+h_{15})k_{13} + h_{12}k_1 + h_{14}k_9 (modp)$ |
| *h'[3,2]* | $h'_{14} = h_{14}(k_2+k_6+k_{10}+k_{14}) + (h_3+h_7+h_{11}+h_{15})k_{14} + h_{12}k_2 + h_{13}k_6 (modp)$ |

**Misol.** $d_2$ – diamatritsaviy ko'paytirish:

$d_2H_1$ $d_2K_1$ $d_2C_1$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \quad @_2 \quad \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv$$

$$\begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

Yuqoridagi diamatritsaga ko'paytirish qoidalaridan foydalanib hisoblangan natijaviy matritsani hisoblashning bitta elementi quyidagicha:

$h'[0,0]=h'_0=h_0(k_0+k_4+k_8+k_{12})-h_5k_4-h_{10}k_8-h_{15}k_{12})(modp)=1*(17+4+9+13)-9*4-6*9-9*13=(43-36-54-117)(mod\ 256)=92.$

Qolgan elementlar ham yuqoridagi jadvaldagi qoidalar asosida hisoblanadi.

So'ngi funksiya *BaytAlmash(Holat,$B_a$)* almashtirishi quyidagi amallarni bajarishdan iborat:

– elementlari bayt sathida berilgan $Holat[8,4]$ massivi elementlari bayt sathida berilgan $Holatb[8,4]$ massivi ko'rinishida nomlanadi;

– agar $m=sh$ bo'lsa, u holda $B_a[256] = B_{sA}[256]$ qabul qilinadi, $Holatb[8,4]$ massivining har bir elementi $B_a$ massivining addresi bo'yicha unga mos elementi bilan almashtiriladi va natijaviy $Holatb[8,4]$ massivi bayt sathida berilgan $Holat[8,4]$ massiviga almashtiriladi, aks holda, ya'ni $m=dsh$ bo'lsa, u holda $B_a[256] = B_{sAD}[256]$ qabul qilinadi, $Holatb[8,4]$ massivining har bir elementi $B_a$ massivining addresi bo'yicha unga mos elementi bilan almashtiriladi va natijaviy $Holat[8,4]$ massivi bayt sathida berilgan $Holat[8,4]$ massiviga almashtiriladi (bu yerda, $s \in \{1,2\}$). Almashtirish natijasining nusxasi *Holat* massiviga ko'chiriladi va shifrmatn sifatida qabul qilinadi.



## 5.6. IDEA simmetrik blokli shifrlash algoritmi

IDEA (ing. International Data Encryption Algorithm – ma'lumotni shifrlashning xalqaro algoritmi) – simmetrik blokli shifrlash algoritmi bo'lib, Shvetsariyaning Ascom firmasi tomonidan patenglangan. Ushbu algoritmning birinchi versiyasi 1990-yilda Lay Syueszya va Djeyms Messi tomonidan PES (ing. Proposed Encryption Standard – taklif etilgan shifrlash standarti) nomi bilan yaratilgan. Ushbu algoritmi Lay-Messi arxitektrurasiga asoslangan.

IDEA algoritmi 128 bitli kalit va 64 bitli blokdan foydalanadi. Raundlar soni 8 ga teng. Ochiq matnlar 64 bitli bloklarga bo'linadi. Agar ochiq matnning bitdagi uzunligi 64 ga karrali bo'lmasa, oxirgi blok aniqlangan baytlar bilan to'ldiriladi. Kiritilgan har bir 64 bitli blok 4 ta teng qismga (16 bitdan) bo'linadi va 16 bitli sonlar ustida shifrlashda foydalanilgan algebraik amallar bajariladi. IDEA shifrlash va rasshifrovkalash uchun yagona algoritmdan foydalanadi.

Algoritmda turli maydonlarda amalga oshiriluvchi quyidagi algebraik amallardan foydalanilgan:

- $2^{16}$ bo'yicha qo'shish amali ($\boxplus$);
- $2^{16}+1$ bo'yicha ko'paytirish amali ($\odot$);
- bitlar ustida bajariluvchi XOR amali ($\oplus$).

Ushbu amallar uchun distributivlik va assotsiativlik qonuni o'rinli emas, ya'ni:

- $a \odot (b \boxplus c) \neq (a \odot b) \boxplus (a \odot c)$;
- $a \boxplus (b \oplus c) \neq (a \boxplus b) \oplus c$.

*Raund kalitlarini generatsiyalash.* 128 bitli kalitdan 8 raundning har biri uchun 16 bitli 6 ta kalit generatsiya qilinadi. Bundan tashqari, 8-raundan so'ng yana 4 ta 16 bitli kalit asosida amallar bajariladi. Umumiy hisobda, $52=8\times6+4$, 16 bitli kalitlar quyidagicha generatsiya qilinadi:

- dastlab 128 bitli kalit 16 bitli qismlarga ajratilib, dastlabki 8 ta qismkalitlarni hosil qiladi: $K_1^{(1)}, K_2^{(1)}, K_3^{(1)}, K_4^{(1)}, K_5^{(1)}, K_6^{(1)}, K_1^{(2)}, K_2^{(2)}$;

- shundan so'ng, 128 bitli kalit chapga 25 bit siklik siljitilib, hosil bo'lgan 128 bitli kalit yuqoridagi kabi 8 ta 16 bitli qismkalitlarga bo'linadi: $K_3^{(2)}, K_4^{(2)}, K_5^{(2)}, K_6^{(2)}, K_1^{(3)}, K_2^{(3)}, K_3^{(3)}, K_4^{(3)}$;

- mazkur ketma-ketlik 52 ta 16 bitli bloklar hosil qilingunga qadar davom ettiriladi.

Natijaviy raund kalitlari esa quyidagicha bo'ladi:

| Raund tartibi | Raundda foydalaniladigan qism kalitlar |
|---|---|
| 1 | $K_1^{(1)}, K_2^{(1)}, K_3^{(1)}, K_4^{(1)}, K_5^{(1)}, K_6^{(1)}$ |
| 2 | $K_1^{(2)}, K_2^{(2)}, K_3^{(2)}, K_4^{(2)}, K_5^{(2)}, K_6^{(2)}$ |
| 3 | $K_1^{(3)}, K_2^{(3)}, K_3^{(3)}, K_4^{(3)}, K_5^{(3)}, K_6^{(3)}$ |
| 4 | $K_1^{(4)}, K_2^{(4)}, K_3^{(4)}, K_4^{(4)}, K_5^{(4)}, K_6^{(4)}$ |
| 5 | $K_1^{(5)}, K_2^{(5)}, K_3^{(5)}, K_4^{(5)}, K_5^{(5)}, K_6^{(5)}$ |
| 6 | $K_1^{(6)}, K_2^{(6)}, K_3^{(6)}, K_4^{(6)}, K_5^{(6)}, K_6^{(6)}$ |
| 7 | $K_1^{(7)}, K_2^{(7)}, K_3^{(7)}, K_4^{(7)}, K_5^{(7)}, K_6^{(7)}$ |
| 8 | $K_1^{(8)}, K_2^{(8)}, K_3^{(8)}, K_4^{(8)}, K_5^{(8)}, K_6^{(8)}$ |
| Chiqish akslantirishi uchun | $K_1^{(9)}, K_2^{(9)}, K_3^{(9)}, K_4^{(9)}$ |

*Shifrlash jarayoni.* IDEA algoritmida ma'lumot blokining shifrlash jarayoni 5.10-rasmda keltirilgan. Shifrlash jarayoni 8 ta raund va chiqish akslantirishidan iborat. Kiritilgan ma'lumot bloki 16 bitli 4 ta qismga ajratiladi ($P_1$, $P_2$, $P_3$, $P_4$). Mazkur 16 bitli bloklar ustida yuqorida keltirilgan uchta amaldan foydalaniladi. Ko'paytirish amalida 0 o'rniga $2^{16}$ foydalaniladi.

Shifrlash algoritmining matematik ifodasi quyida keltirilgan:

-64 bitli blok 16 bitli qismbloklarga ajratiladi ($P_1^{(0)}, P_2^{(0)}, P_3^{(0)}, P_4^{(0)}$);

-har bir raund uchun ($i = 1 \cdots 8$) quyidagilar bajariladi:

- $A^{(i)} = P_1^{(i-1)} \odot K_1^{(i)}$;
- $B^{(i)} = P_2^{(i-1)} \boxplus K_2^{(i)}$;
- $C^{(i)} = P_3^{(i-1)} \boxplus K_3^{(i)}$;
- $D^{(i)} = P_4^{(i-1)} \odot K_4^{(i)}$;
- $E^{(i)} = A^{(i)} \oplus C^{(i)}$;
- $F^{(i)} = B^{(i)} \oplus D^{(i)}$;
- $P_1^{(i)} = A^{(i)} \oplus ((F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)})$;
- $P_2^{(i)} = C^{(i)} \oplus ((F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)})$;



- $P_3^{(i)} = B^{(i)} \oplus (E^{(i)} \odot K_5^{(i)} \boxplus (F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)})$;
- $P_4^{(i)} = D^{(i)} \oplus (E^{(i)} \odot K_5^{(i)} \boxplus (F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)})$.

Yuqorida keltirilgan amallar 8 raund bajarilgandan so'ng, natijaviy 4 ta 16 bitli bloklar $P_1^{(8)}, P_2^{(8)}, P_3^{(8)}, P_4^{(8)}$ ga teng bo'ladi.

Shundan so'ng, natijaviy akslantirish quyidagicha amalga oshiriladi ($i = 9$):

- $P_1^{(9)} = P_1^{(8)} \odot K_1^{(9)}$;
- $P_2^{(9)} = P_3^{(8)} \boxplus K_2^{(9)}$;
- $P_3^{(9)} = P_2^{(8)} \boxplus K_3^{(9)}$;
- $P_4^{(9)} = P_4^{(8)} \odot K_4^{(9)}$.

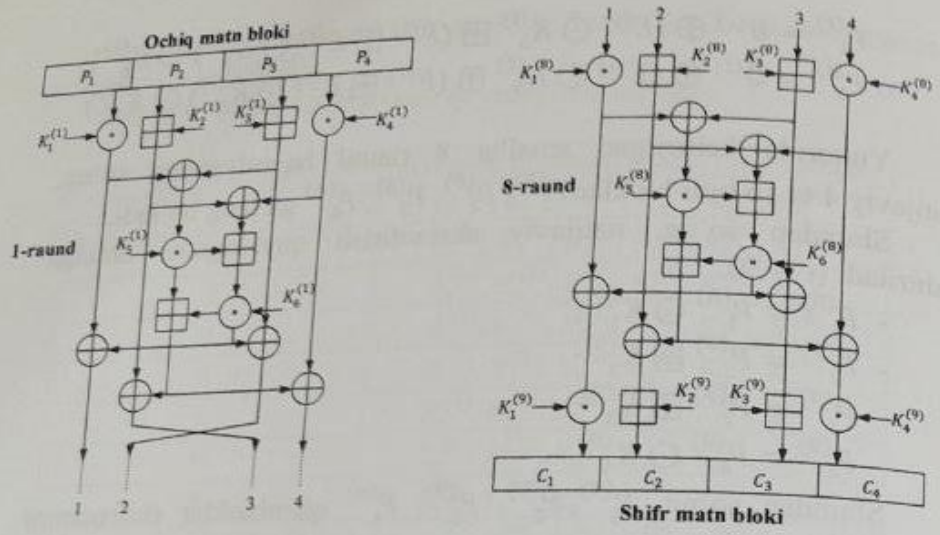
Shundan so'ng, $P_1^{(9)}, P_2^{(9)}, P_3^{(9)}, P_4^{(9)}$ qismbloklar shifrmatnni hosil qiladi.

*Rasshifrovkalash jarayoni.* Rasshifrovkalash jarayoni ham 5.10-rasmda keltirilgan kabi amalga oshiriladi. Faqat, raund kalitlari teskari tartibda foydalaniladi. Rasshifrovkalash uchun raund kalitlarini teskari foydalanish tartibi 5.10-jadvalda keltirilgan.

*5.10-jadval*

Rasshifrovkalash uchun raund kalitlarining tartibi

| **Raund tartibi** | **Raundda foydalaniladigan qism kalitlar** |
|---|---|
| 1 | $1/K_1^{(9)}, -K_2^{(9)}, -K_3^{(9)}, 1/K_4^{(9)}, K_5^{(8)}, K_6^{(8)}$ |
| 2 | $1/K_1^{(8)}, -K_3^{(8)}, -K_2^{(8)}, 1/K_4^{(8)}, K_5^{(7)}, K_6^{(7)}$ |
| 3 | $1/K_1^{(7)}, -K_3^{(7)}, -K_2^{(7)}, 1/K_4^{(7)}, K_5^{(6)}, K_6^{(6)}$ |
| 4 | $1/K_1^{(6)}, -K_3^{(6)}, -K_2^{(6)}, 1/K_4^{(6)}, K_5^{(5)}, K_6^{(5)}$ |
| 5 | $1/K_1^{(5)}, -K_3^{(5)}, -K_2^{(5)}, 1/K_4^{(5)}, K_5^{(4)}, K_6^{(4)}$ |
| 6 | $1/K_1^{(4)}, -K_3^{(4)}, -K_2^{(4)}, 1/K_4^{(4)}, K_5^{(3)}, K_6^{(3)}$ |
| 7 | $1/K_1^{(3)}, -K_3^{(3)}, -K_2^{(3)}, 1/K_4^{(3)}, K_5^{(2)}, K_6^{(2)}$ |
| 8 | $1/K_1^{(2)}, -K_3^{(2)}, -K_2^{(2)}, 1/K_4^{(2)}, K_5^{(1)}, K_6^{(1)}$ |
| Chiqish akslantirishi uchun | $1/K_1^{(1)}, -K_2^{(1)}, -K_3^{(1)}, 1/K_4^{(1)}$ |




*5.10-rasm.* **IDEA algoritmining shifrlash jarayoni**

Bu yerda, $1/K_j^{(i)}$ qism kalit $K_j^{(i)}$ kalitning $2^{16}+1$ maydondagi multiplikativ teskarisi bo'lib, ular uchun $1/K_j^{(i)} * K_j^{(i)} = 1 mod(2^{16}+1)$ tenglik o'rinli bo'ladi. $-K_j^{(i)}$ qism kalit esa $K_j^{(i)}$ kalitning teskarisi bo'lib, ular uchun $-K_j^{(i)} + K_j^{(i)} = 0 mod(2^{16})$ tenglik o'rinli. Masalan, $K_1^{(9)} = 0x0080$ ga teng bo'lsa, $1/K_1^{(9)} = 0xfe01$ ga teng bo'ladi, yoki $K_2^{(9)} = 0x00c0$ uchun $-K_2^{(9)} = 0xff40$ ga teng bo'ladi.

Ushbu algoritm shifrlash jarayonida yuqori tezlik qayd etib, apparat tarzda amalga oshirishga qulay hisoblanadi. Xususan, IDEA algoritmi DES algoritmiga nisbatan 2 marta tezkor va xavfsizlik nuqtai nazaridan bardoshli hisoblanadi.

### 5.7. Twofish simmetrik blokli shifrlash algoritmi

Twofish algoritmi ma'lumotni shifrlashda 128 bitli ochiq matn bloki, 128, 192 va 256 bitli kalitlardan foydalanadi. Raundlar soni esa 16 ga teng bo'lib, Bryus Shnayer boshchiligidagi kriptogriflar tomonidan 1998-yilda ishlab chiqilgan. Ushbu algoritm AES konkursining 2 raundida ishtirok etgan 5 ta algoritmdan biri

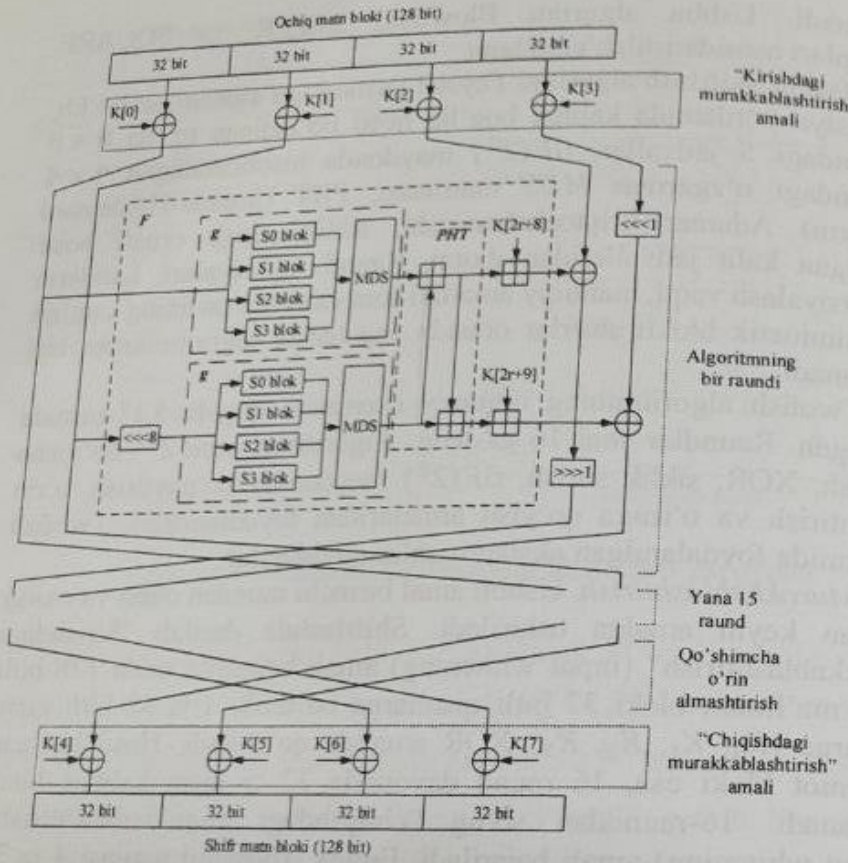


hisoblanadi. Ushbu algoritm Blowfish, SAFER va SQUARE algoritmlari asosida ishlab chiqilgan.

Mazkur shifrlash algoritmi Feystel tarmog'iga asoslangan bo'lib, $F$ funksiya yordamida kalitga bog'liq hosil bo'ladigan to'rtta $8 \times 8$ o'lchamdagi $S$ jadvallar, $GF(2^8)$ maydonda hisoblanadigan $4 \times 4$ o'lchamdagi o'zgarmas $MDS$ matritsasi, PHT (pseuda-HAdamard transform) Adamar kriptoakslantirishi, siklik surish orqali hosil bo'ladigan kalit jadvallaridan iborat. Raund funksiyalari, kalitlarni generatsiyalash vaqti, mantiqiy amallari soni va xotira sarfining kamligi bilan simmetik blokli shifrlar orasida eng tezkor algoritmlardan biri hisoblanadi.

Twofish algoritmining umumiy sxemasini quyida 5.11-rasmda keltirilgan. Raundlar soni 16 ga teng. Algoritmda $mod\ 2^{32}$ bo'yicha qo'shish, XOR, siklik surish, $GF(2^8)$ maydonida ko'paytirish, o'rin almashtirish va o'rniga qo'yish amallaridan foydalanilgan. Twofish algoritmida foydalanilgan akslantirishlar quyidagilar.

*Murakkablashtirish.* Ushbu amal birinchi raundan oldin va oxirgi raundan keyin amalga oshiriladi. Shifrlashda dastlab "kirishdagi murakkablashtirish" (input whitening) amali bajarilib, unda 128 bitli ochiq ma'lumot bloki 32 bitli qismlarga bo'linib, 4 ta 32 bitli qism kalitlarga ($K_0$, $K_1$, $K_2$, $K_3$) XOR amalida qo'shiladi. Hosil bo'lgan ma'lumot bloki esa, 16 raund davomida 32 ta qism kalitlar bilan shifrlanadi. 16-raunddan so'ng "chiqishdagi murakkablashtirish" (output whitening) amali bajariladi. Bunda, 16-raund natijasi 4 ta 32 bitli qismlarga ajratilib, 4 ta 32 bitli qism kalitlar ($K_4$, $K_5$, $K_6$, $K_7$) bilan XOR amalida qo'shiladi.




*5.11-rasm.* **Twofish algoritmining shifrlash jarayoni sxemasi**

*g funksiya.* $g$ funksiya Twofish algoritmining asosi hisoblanadi. Ushbu funksiya kirishida 32 bitli ma'lumot $X$ qabul qilinadi va u 4 baytga $x_0$, $x_1$, $x_2$, $x_3$ baytlarga ajratiladi. Har bir bayt o'ziga biriktirilgan $S$ bloklardan ($S$ bloklar statik emas, kalitga bog'liq holda o'zgaradi) o'tkaziladi. $S$ jadvaldan olingan 4 bayt vektor sifatida talqin qilinib, 4×4 o'lchamli statik MDS (maximum distance separable) matritsaga $GF(2^8)$ maydonida $x^8 + x^6 + x^5 + x^3 + 1$ modul bo'yicha ko'paytiriladi. Twofish algoritmida foydalanilgan MDS matritsa quyida keltirilgan bo'lib, kirishda bir baytning o'zgarishi chiqishdagi 4 baytning o'zgarishini ta'minlaydi.



$$MDS = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{pmatrix}$$

*Adamar kriptoakslantirishi.* Ushbu akslantirish $2n$ uzunlikdagi bitlar qatorini qayta akslantirishni amalga oshiradi. Qator dastlab, $n$ bitdan bo'lgan ikkita $a$, $b$ qismlarga ajratiladi. Akslantirish quyidagicha amalga oshiriladi:

$$a' = a + b(mod\ 2^n);$$
$$b' = a + 2b(mod\ 2^n).$$

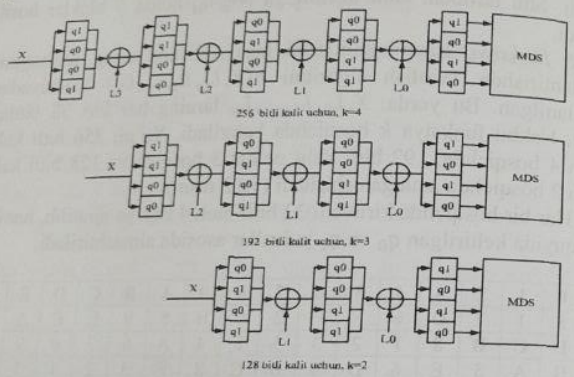
Mazkur akslantirish ko'plab algoritmlarda foydalanilgan (masalan, SAFER) bo'lib, Twofish algoritmi uchun $n = 32$ ga teng.

*Siklik 1 bitga surish.* Har bir raund uchun $F$ funksiyaning natijasi o'ng tomondagi ikki tashkil etuvchilar bilan XOR amalda qo'shilgandan so'ng (va oldin), qo'shimcha tarzda bir bitga siklik siljitiladi. Xususan, uchinchi blok XOR amalidan so'ng o'nga bir bit, to'rtinchi blok esa XOR amalidan oldin chapga bir bit siklik siljitiladi. Ushbu siljitishlar $S$ jadvallar va $MDS$ matritsaga xos bo'lgan baytlar bo'yicha nomutanosiblikni bartaraf etish uchun maxsus qo'shilgan. Rasshifrovkalash jarayonida esa, siljitishlar qarama-qarshi yo'nalishda amalga oshiriladi.

*Raund kalitlari va S bloklarni generatsiyalash.* Twofish algoritmida $N=128$, $N=192$ va $N=256$ bitli kalitdan foydalanish mumkin. Kirish kalitining 256 bitdan kichik ixtiyoriy qiymatida 0 bilan to'ldirilib, keyingi aniqlangan kalit uzunligiga yetkaziladi. Kiruvchi kalitdan 40 ta 32 bitli qism kalitlar generatsiya qilinadi: ularning dastlabki 8 tasi "kirishdagi murakkablashtirish" va "chiqishdagi murakkablashtirish" uchun, qolgan 32 tasi esa har bir raunda 2 tadan foydalaniladi. Twofish algoritmida kiruvchi kalit nafaqat raund kalitlarini generatsiyalashda, balki S jadvallarni hosil qilishda ham ishlatiladi.

$b_2 = t_1[b_1];$
$a_3 = a_2 \oplus b_2;$
$b_3 = a_1 \oplus (b_2 >>> 2) \oplus ((8a_2) mod 16);$
$a_4 = t_2[a_3];$
$b_4 = t_3[b_3];$
$y = 16b_4 + a_4.$

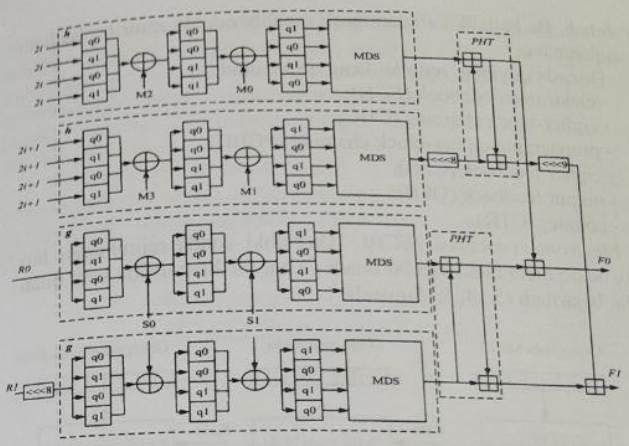
Shundan so‘ng, $y$ qiymatlar 4 baytli vektor sifatida akslantirilib, yuqorida keltirilgan MDS matritsaga ko‘paytiriladi.




*5.12-rasm.* **Turli kalit uzunliklari uchun $h$ funksiyaning ko‘rinishi**

Yuqorida keltirilgan akslantirishlardan kelib chiqib, Twofish algoritmida 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi 5.13-rasmda keltirilgan.






*5.13-rasm.* **Twofish algoritmida 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi**

Bu yerda, $R_0, R_1$ bloklar $F$ raund funksiyasiga kiritiladi va mos $F_0, F_1$ qiymatlar olinadi.

### 5.8. Simmetrik blokli shifrlash rejimlari

Oqimli shifrlardan foydalanish juda ham sodda – ochiq matn (yoki shifrmatn) uzunligiga teng bo‘lgan kalitlar ketma-ketligi generatsiya qilinadi va XOR amalida bajariladi. Blokli shifrlardan foydalanish faqat bir blokni shifrlashda oson. Biroq, bir nechta (ko‘plab) bloklarni shifrlash qanday amalga oshiriladi? Javob esa, bir qaraganda oson emas.

Shu sababli, simmetrik blokli shifrlardan turli ko‘rinishlarda (rejimlarda) foydalanishga harakat qilinadi. Aksariyat rejimlarda amalga boshlang‘ich vektor (initialization vector, IV) dan foydalaniladi. Boshlang‘ich vektor ma’lum bitlar ketma-ketligidan iborat bo‘lib, ochiq matnga yoki kalitga ma’lum algoritm bo‘yicha

$k = N/64$ kabi belgilaylik. U holda $M$ kirish kaliti $8k$ baytdan, $m_0, \ldots, m_{8k-1}$, iborat bo'ladi. Baytlar dastlab $2k$ ta 32 bitli so'zlarga ajratiladi:

$$M_i = \sum_{j=0}^{3} m_{(4i+j)} \cdot 2^{8j}, \quad i = 0, \ldots, 2k-1.$$

Shundan so'ng ular, $k$ uzunlikdagi ikkita vektorga ajratiladi:

$$M_e = (M_0, M_2, \ldots, M_{2k-2});$$
$$M_o = (M_1, M_3, \ldots, M_{2k-1}).$$

$M_e$ va $M_o$ asosida 40 ta qism kalitlar quyidagicha hosil qilinadi:

$$p = 2^{24} + 2^{16} + 2^8 + 2^0;$$
$$A_i = h(2ip, M_e);$$
$$B_i = h((2i+1)p, M_o) \lll 8;$$
$$K_{2i} = (A_i + B_i) mod 2^{32};$$
$$K_{2i+1} = ((A_i + 2B_i) mod 2^{32}) \lll 9.$$

Bu yerda, $i = 0, \ldots, 19$ bo'lib, umumiy 40 ta qism kalitlarni generatsiyalash imkonini beradi. $2ip$ – belgilanish esa, $2i$ qiymatni 4 marta takrorlanishini bildiradi, ya'ni, $2ip = 2i \parallel 2i \parallel 2i \parallel 2i$. $h$ funksiyaning tavsifi esa quyida keltiriladi.

Uzunligi $k$ ga teng $S$ bloklarni generatsiyalash uchun kiruvchi kalitdan foydalaniladi. Buning uchun kiruvchi kalit uzunligi 8 ga teng baytdan tashkil topgan guruhlarga bo'linadi. Masalan, 128 bitli kalit uchun birinchi guruh $m_0, \ldots, m_7$ dan iborat bo'lsa, ikkinchi guruh esa $m_8, \ldots, m_{15}$ elementlardan iborat bo'ladi. Har bir guruh vektor shaklida ifodalanib, Reed Solomon kodida foydalanilgan 4×8 o'lchamli matritsaga $GF(2^8)$ maydonida $x^8 + x^6 + x^3 + x^2 + 1$ modul bo'yicha ko'paytiriladi.



$$\begin{bmatrix} s_{i,0} \\ s_{i,1} \\ s_{i,2} \\ s_{i,3} \end{bmatrix} = \begin{bmatrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{bmatrix} \cdot \begin{bmatrix} m_{8i} \\ m_{8i+1} \\ m_{8i+2} \\ m_{8i+3} \\ m_{8i+4} \\ m_{8i+5} \\ m_{8i+6} \\ m_{8i+7} \end{bmatrix}$$

Bitta guruh uchun hosil qilingan $S_i = \sum_{j=0}^{3} s_{i,j} \cdot 2^{8j}$ ga teng bo'ladi. Shu tartibda, kalit uzunligiga bog'liq holda $S$ bloklar hosil qilinadi.

*h funksiya.* Raund kalitlarini hosil qilishda va $g$ funksiyani shakllantirishda Twofish algoritmi $h(X, L_0, L_1, \ldots, L_k)$ funksiyadan foydalanilgan. Bu yerda, $X, L_0, L_1, \ldots, L_k$ larning har biri 32 bitdan iborat. Ushbu funksiya $k$ bosqichda bajariladi. Ya'ni, 256 bitli kalit uchun 4 bosqichda, 192 bitli kalit uchun 3 bosqich va 128 bitli kalit uchun 2 bosqichda amalga oshiriladi (5.12-rasm).

Har bir bosqichda kiruvchi 32 bitli blok 4 baytga ajratilib, har bir bayt quyida keltirilgan $q_0$ va $q_1$ jadvallar asosida almashtiriladi.

| $q_0$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t_0$ | 8 | 1 | 7 | D | 6 | F | 3 | 2 | 0 | B | 5 | 9 | E | C | A | 4 |
| $t_1$ | E | C | B | 8 | 1 | 2 | 3 | 5 | F | 4 | A | 6 | 7 | 0 | 9 | D |
| $t_2$ | B | A | 5 | E | 6 | D | 9 | 0 | C | 8 | F | 3 | 2 | 4 | 7 | 1 |
| $t_3$ | D | 7 | F | 4 | 1 | 2 | 6 | E | 9 | B | 3 | 0 | 8 | 5 | C | A |

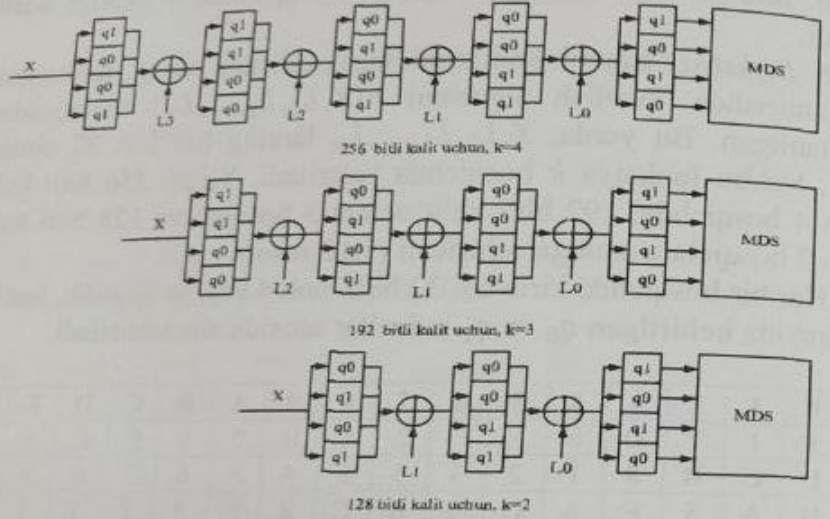
| $q_1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t_0$ | 2 | 8 | B | D | F | 7 | 6 | E | 3 | 1 | 9 | 4 | 0 | A | C | 5 |
| $t_1$ | 1 | E | 2 | B | 4 | C | 3 | 7 | 6 | D | A | 5 | F | 9 | 0 | 8 |
| $t_2$ | 4 | C | 7 | 5 | 1 | 6 | 9 | A | 0 | E | D | 8 | 2 | B | 3 | F |
| $t_3$ | 8 | 9 | 5 | 1 | C | 3 | D | E | 6 | 4 | 7 | F | 2 | 0 | 8 | A |

Buning uchun, kiruvchi bayt $x$ ikkita 4 bitli $a_0 = \lfloor x/16 \rfloor$ va $b_0 = x \, mod 16$ qismlarga ajratiladi hamda ular ustida quyidagi amallar bajariladi:

$$a_1 = a_0 \oplus b_0;$$
$$b_1 = a_0 \oplus (b_0 \ggg 4) \oplus ((8a_0) mod 16);$$
$$a_2 = t_0[a_1];$$

$b_2 = t_1[b_1];$
$a_3 = a_2 \oplus b_2;$
$b_3 = a_1 \oplus (b_2 \ggg 2) \oplus ((8a_2) mod 16);$
$a_4 = t_2[a_3];$
$b_4 = t_3[b_3];$
$y = 16b_4 + a_4.$

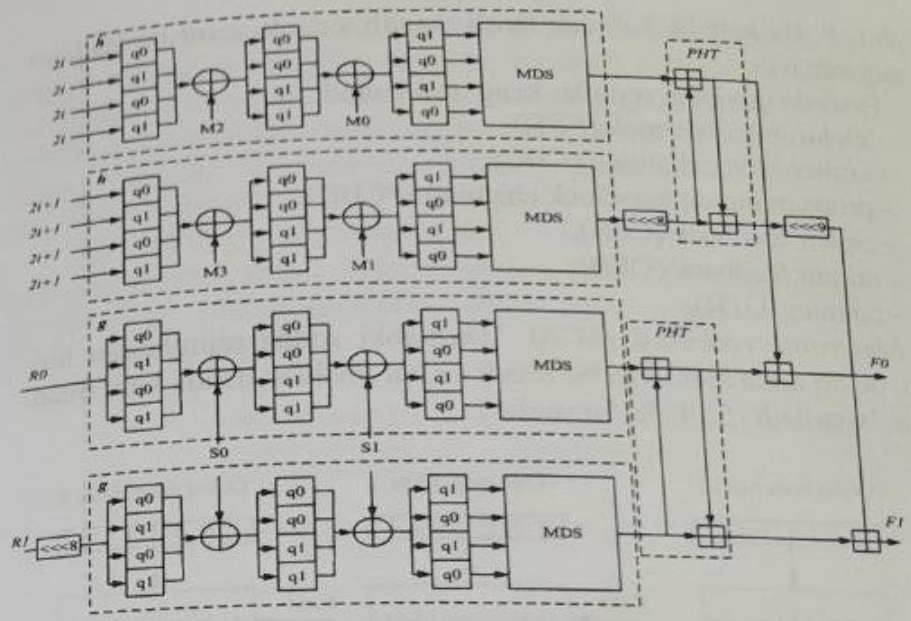
Shundan so‘ng, $y$ qiymatlar 4 baytli vektor sifatida akslantirilib, yuqorida keltirilgan MDS matritsaga ko‘paytiriladi.




*5.12-rasm.* **Turli kalit uzunliklari uchun *h* funksiyaning ko‘rinishi**

Yuqorida keltirilgan akslantirishlardan kelib chiqib, Twofish algoritmida 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi 5.13-rasmda keltirilgan.






*5.13-rasm.* **Twofish algoritmida 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi**

Bu yerda, $R_0, R_1$ bloklar $F$ raund funksiyasiga kiritiladi va mos $F_0, F_1$ qiymatlar olinadi.

## 5.8. Simmetrik blokli shifrlash rejimlari

Oqimli shifrlardan foydalanish juda ham sodda – ochiq matn (yoki shifrmatn) uzunligiga teng bo‘lgan kalitlar ketma-ketligi generatsiya qilinadi va XOR amalida bajariladi. Blokli shifrlardan foydalanish faqat bir blokni shifrlashda oson. Biroq, bir nechta (ko‘plab) bloklarni shifrlash qanday amalga oshiriladi? Javob esa, bir qaraganda oson emas.

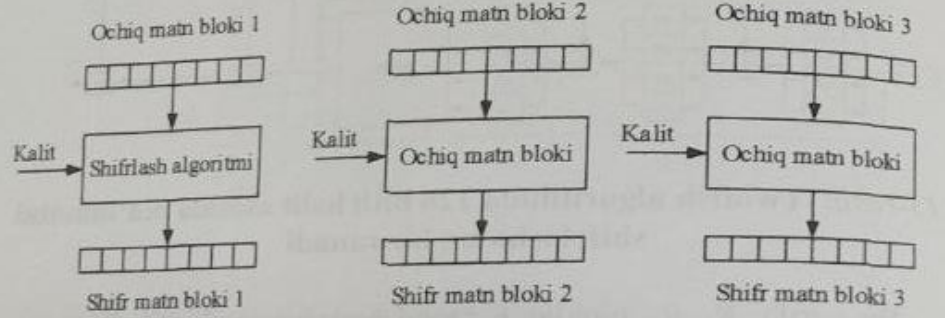
Shu sababli, simmetrik blokli shifrlardan turli ko‘rinishlarda (rejimlarda) foydalanishga harakat qilinadi. Aksariyat rejimlarda amalga boshlang‘ich vektor (initialization vector, IV) dan foydalaniladi. Boshlang‘ich vektor ma’lum bitlar ketma-ketligidan iborat bo‘lib, ochiq matnga yoki kalitga ma’lum algoritm bo‘yicha

qo'shiladi. Bu kattalik kalitdan farqli sanalib, odatda zarur bo'lsa ham sir saqlanmaydi.

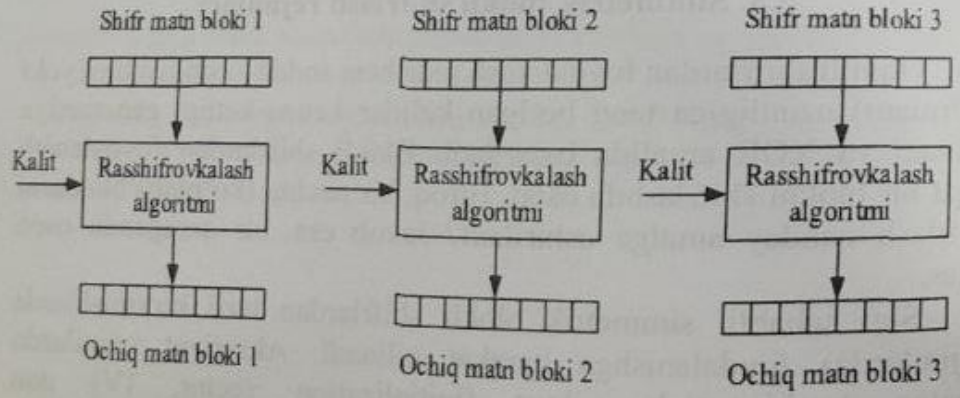
Hozirda quyidagi rejimlar keng qo'llaniladi:

- elektronic codebook (ECB);
- cipher-block chaining (CBC);
- propagating cipher-block chaining (PCBC);
- cipher feedback (CFB);
- output feedback (OFB);
- counter (CTR).

*Electronic codebook (ECB).* Dastlabki sodda rejimlardan biri bo'lib, ochiq matn bloklarga bo'linadi va har bir blok ustida kalit bilan amallar bajariladi (5.14, 5.15-rasmlar).




*5.14-rasm.* **ECB rejimida shifrlash**

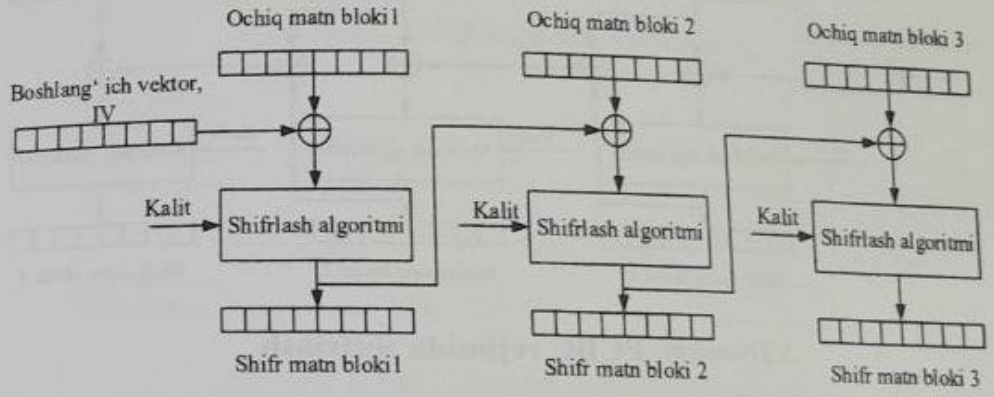



*5.15-rasm.* **ECB rejimida rasshifrovkalash**

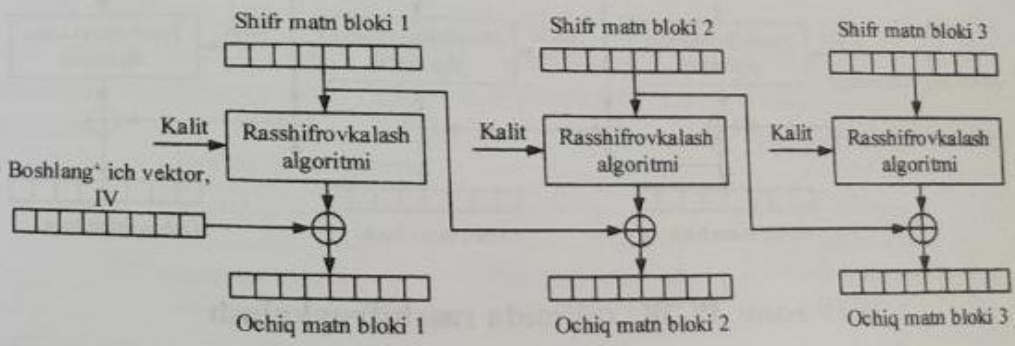


Ushbu rejimning asosiy kamchiligi bir xil ochiq matn bir xil shifr matnga almashadi. Bundan tashqari, bu rejim matnni yashirish kabi vazifalarni bajarmaydi. Shularni hisobga olgan holda o'ta maxfiy axborot bilan ishlashda ushbu rejimdan foydalanish tavsiya etilmaydi. Biroq, dasturiy ko'rinishda parallel ravishda amalga oshirish imkoniyati mavjud.

*Cipher-block chaining (CBC).* Ushbu rejim 1976-yil IBM kompaniyasi tomonidan ishlab chiqilgan bo'lib, dastlab ochiq matnga boshlang'ich vektor qo'shilib, natija kalit yordamida shifrlanadi (5.16, 5.17-rasmlar).




*5.16-rasm.* **CBC rejimida shifrlash**

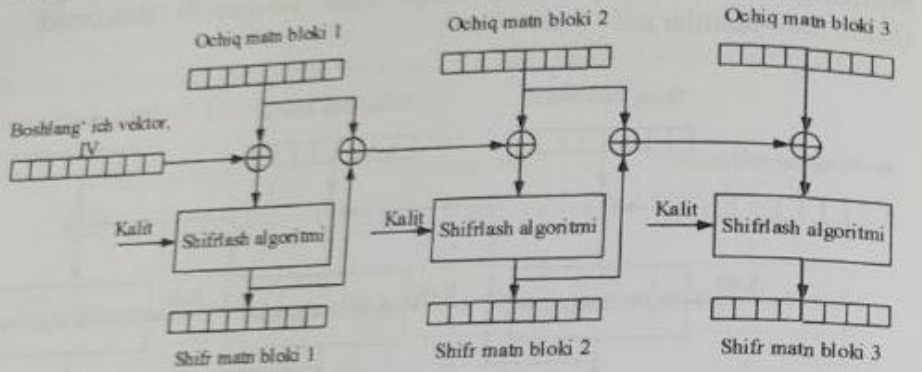



*5.17-rasm.* **CBC rejimida rasshifrovkalash**

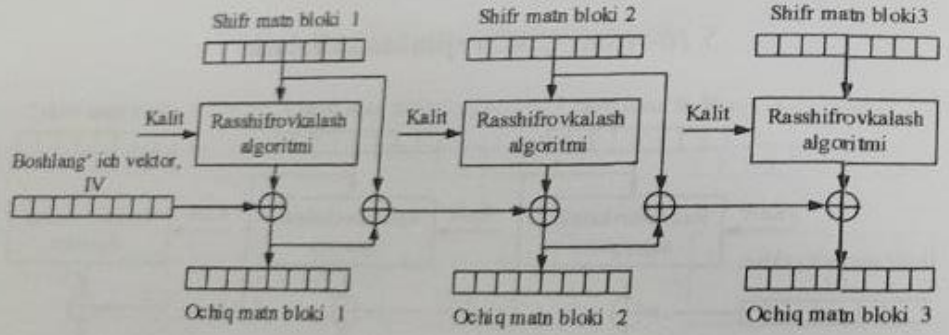
Ushbu rejimda shifrlashda bir xil ma'lumot bloklari har xil shifrmatn bloklariga almashtiriladi. Bu esa shifrmatnga qarab tahlil

qilish usulini oldini olishga yordam beradi. Keyingi bosqich natijasi oldingi bosqich natijasiga bog'liq bo'lgani bois, algoritmni parallel tarzda amalga oshirish mumkin emas.

*Propagating cipher-block chaining (PCBC).* Ushbu rejim Kerberosv4 va WASTE protakollarida foydalanilgan bo'lsada, bardoshlsizligi sababli amalda keng qo'llanilmaydi. Bundan tashqari, ushbu rejim parallel amalga oshirish imkoniyatini bermaydi (5.18, 1.19-rasmlar).




*5.18-rasm.* **PCBC rejimida shifrlash**

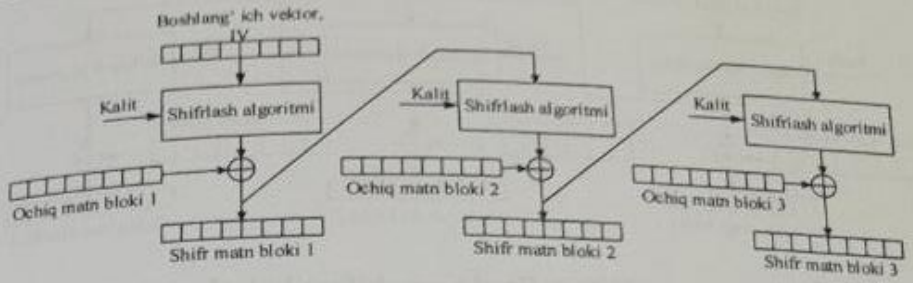



*5.19-rasm.* **PCBC rejimida rasshifrovkalash**

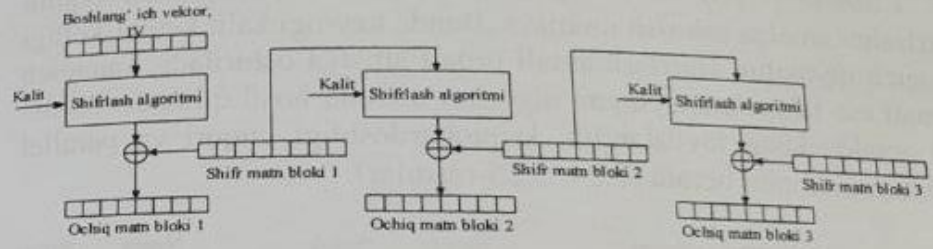
*Cipher feedback (CFB).* Ushbu rejim CBC rejimiga yaqin bo'lib, ushbu modelda rasshifrovkalash CBC modelida shifrlash amaliga o'xshaydi. Ushbu rejimda rasshifrovkalashda ham shifrlash amalidan



foydalaniladi. Ushbu rejimni ham dasturiy tomondan parallel amalga oshirish imkoniyati mavjud emas (5.20, 5.21-rasmlar).

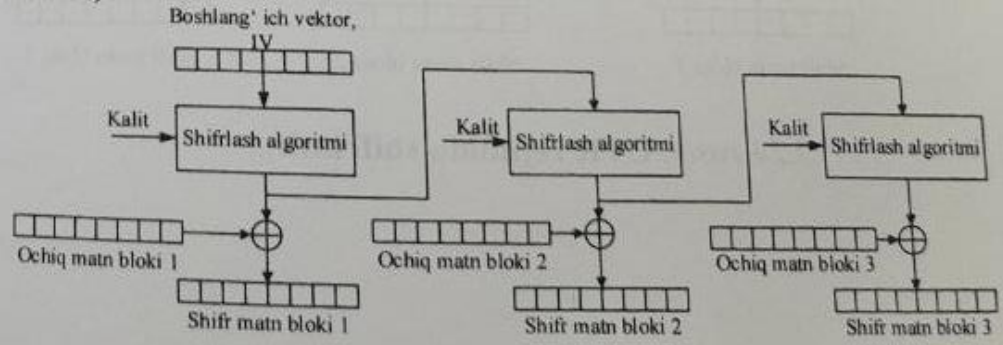



*5.20-rasm.* **CFB rejimda shifrlash**

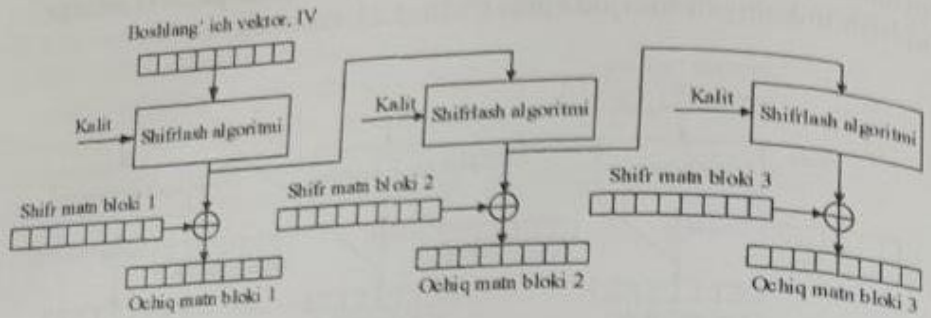



*5.21-rasm.* **CFB rejimda rasshifrovkalash**

*Output feedback (OFB).* Ushbu rejimda shifrlash amali sinxron oqimli shifrlash algoritmlarini qurishga imkon beradi. Ushbu rejimda shifrlashda keyingi blok oldingi blokga bog'liq bo'lganligi sababli, parallel ravishda amalga oshirish imkoniyati mavjud emas (5.22, 5.23-rasmlar).

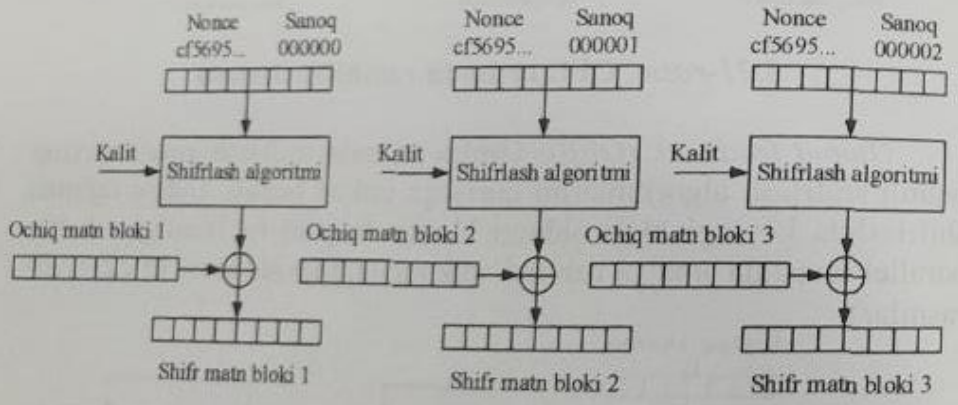



*5.22-rasm.* **OFB rejimda shifrlash**



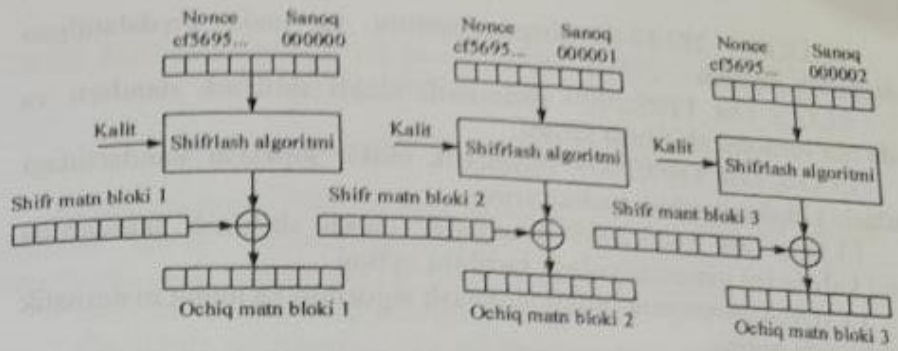

*5.23-rasm.* **OFB rejimda rasshifrovkalash**

*Counter (CTR).* OFB rejimi kabi ushbu rejimda ham oqimli shifrlashni amalga oshirish mumkin. Bunda keyingi kalit ketma-ketligi sanagich qiymatini shifrlash amali orqali amalga oshiriladi. Sanagich qiymati esa takrorlanmaydigan algoritm asosida hosil qilinadi. Ushbu usul amalda keng foydalanilib, kriptobardoshligi yuqori va parallel hisoblash imkonini beradi (5.24, 5.25-rasmlar).




*5.24-rasm.* **CTR rejimida shifrlash**






*5.25-rasm.* **CTR rejimida rasshifrovkalash**

Yuqoridagi rasmlardan ko‘rinib turibdiki, ba’zi shifrlash rejimlarida ham shifrlash ham rasshifrovkalash amallari birgalikda amalga oshirilsa, ba’zida faqat shifrlash amalidan foydalaniladi.

### Navorat savollari

1. Simmetrik blokli shifrlarga oid asosiy tushunchalarni ayting.
2. Zamonaviy blokli shifrlash algoritmlari yaratilish asosiga ko‘ra qanday turlarga bo‘linadi.
3. Feystel tarmog‘i va uning xususiyatlari haqida gapiring.
4. SPN tarmoq va unda foydalanilgan akslantirishlar haqida ma’lumot bering.
5. Lai-Massey tarmog‘iga asoslangan shifrlarni o‘ziga xos xususiyatlarini ayting.
6. DES algoritmi va unda ma’lumotni shifrlash tartibini tushuntiring.
7. DES algoritmida raund kalitlarini generatsiyalash tartibini ayting.
8. AES shifrlash algoritmi va uning matematik asosi haqida ayting.
9. AES shifrlash algoritmida ma’lumotni shifrlash tartibini tushuntiring.
10. AES shifrlash algoritmida raund kalitlarini generatsiyalash tartibini ayting.

11. GOST 28147-89 kriptoalgoritmi va unda foydalanilgan matematik amallar.

12. O'z Dst 1105:2009 simmetrik blokli shifrlash standarti va unda ma'lumotni shifrlash tartibi.

13. O'z Dst 1105:2009 simmetrik blokli shifrlash standartidagi Aralash() akslantirishini tushuntiring.

14. O'z Dst 1105:2009 simmetrik blokli shifrlash standartida raund kalitlarini generatsiyalash tartibini ayting.

15. IDEA simmetrik blokli shifrlash algoritmi va uning matematik asosi haqida ayting.

16. Twofish simmetrik blokli shifrlash algoritmi va uning matematik asosi.

17. Twofish simmetrik blokli shifrlash algoritmida raund kalitlari va S jadvallarni generatsiyalash tartibini tushuntiring.

18. Simmetrik blokli shifrlash rejimlari nima va ularning vazifasi.

19. CTR shifrlash rejimi va uning afzalliklari.

20. CBC shifrlash rejimi va uning afzalliklari.



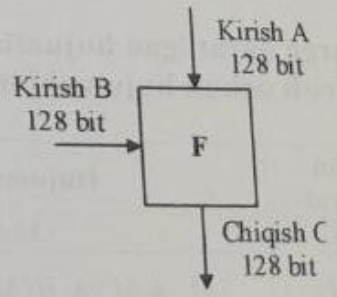
# 6 BOB.
# XESH FUNKSIYALAR VA MA'LUMOTNING YAXLITLIGI TA'MINLASH

## 6.1. Xesh funksiyalar va ularni qurish usullari

Xesh funksiya kirishdagi cheklanmagan uzunlikdagi ma'lumotni chiqishda qat'iy uzunlikdagi qiymatga akslantiruvchi funksiya. Kriptografik xesh funksiyaga quyidagi talablar qo'yiladi:

1. Ixtiyoriy uzunlikdagi matnga qo'llash.
2. Chiqishda tayinlangan uzunlikdagi qiymatni qaytarish.
3. Berilgan ixtiyoriy $x$ bo'yicha $h(x)$ oson hisoblanishi.
4. Berilgan ixtiyoriy $H$ bo'yicha $h(x) = N$ tenglikdan $x$ ni hisoblab topib bo'lmaslik (bir tomonlilik xossasi).
5. Olingan $x$ va $y \neq x$ matnlar uchun $h(x) \neq h(y)$ bajarilishi (kolliziyaga bardoshlilik xossasi).

*Siqish funksiyasi.* Xesh funksiyalarning asosiy xususiyatlaridan biri bu – siqish imkoniyati bo'lib, kriptografiyada bu – fiksirlangan ikkita kiruvchi bloklarni, chiqishda bitta fiksirlangan blokga aylantirib beruvchi bir tomonlama funksiyaga aytiladi (6.1-rasm).




*6.1 – rasm.* **Bir tomonlama siqish funksiyasi**

Bir tomonlama siqish funksiyalarni ishlab chiqishda ba'zida mavjud kriptografik algoritmlardan foydalanilsa, ba'zida biror matematik muammodan kelib chiqqan holda yondashiladi. Quyida keng tarqalgan bir tomonlama siqish funksiyalarini yaratish usullari keltirilgan:

1. Blokli shifrlarga asoslangan:

a) bitta blok uzunligiga siqish:

- Davies-Meyer (Davies-Meyer);
- Matias-Meyer-Oseas (Matyas-Meyer-Oseas);
- Miaguchi-Prinel (Miyaguchi-Preneel).

b)ikkita blok uzunligiga siqish:
- MDC-2;
- MDC-4;
- Hirose.

2. Oqimli shifrlarga asoslangan;
3. Maxsus siqishga asoslangan;
4. Modul arifmetikasiga asoslangan.

***Xesh funksiyalarga qaratilgan hujumlar.*** Xesh funksiyalarni xavfsizlik xususiyatlarini tahlil qilganda odatda *haqiqiy* ma'lumotni topish, *ikkilamchi haqiqiy* ma'lumotni topish va *kolliziyani* topishga qaratiladi. Agar haqiqiy ma'lumotni topish, ikkilamchi haqiqiy ma'lumotni topish va kolliziyani topish uchun mos ravishda $2^n$, $2^n$ va $2^{n/2}$ dan kam bo'lgan urinishlar soni talab etilsa, bu xesh funksiya ko'rsatilgan turdagi hujumlarga bardoshsiz deb qaraladi. Xesh funksiyalarga qaratilgan hujumlarni maqsadiga ko'ra quyidagicha ifodalash mumkin (6.1 - jadval).

*6.1 – jadval*

**Xesh funksiyalarga qaratilgan hujumlarning maqsad va uni amalga oshirish uchun hujumchi imkoniyatlari**

| Hujum | Berilgan imkoniyat | Hujumdan maqsad |
|---|---|---|
| Haqiqiy | $H(M)$ | $M$ ni topish |
| Ikkilamchi haqiqiy | $M\&H(M)$ | $M' \neq M$ va $H(M') \neq H(M)$ ni topish |
| Kolliziya | - | $M' \neq M$ va $H(M') \neq H(M)$ ni topish |

*Tug'ilgan kun hujumi.* Ushbu hujum kolliziyani topishga ratilgan bo'lib, *tug'ilgan kun muammosi* yoki *tug'ilgan kun radoksi*ga asoslanadi. Bu muammo minimal sondagi odamlar orasida nida ikkita odamning tug'ilgan kunining bir xil bo'lish ehtimoli ½ katta bo'lishi haqida bo'lib, buni xesh funksiyalarga qo'llaganda tug'ilgan kunga ega bo'lgan ikkita insonning mavjudligini bildiradi.



Ushbu hujumda hujumchi maxsus kolliziyani topishdan ko'ra ixtiyoriy kolliziyani topishga harakat qiladi. Agar hujumchi $N$ ta odamlar orasidan biror maxsus kolliziyani, ya'ni bir odamning tug'ilgan kuni bilan bir xil bo'lgan kunni topayotgan bo'lsa, u holda bu ehtimol quyidagiga teng bo'ladi:

$$P_{kolliziya}(N) = 1 - \left(\frac{364}{365}\right)^N$$

Bu ehtimollik ½ dan katta bo'lishi uchun $N$ qiymat 254 dan katta bo'lishi talab etiladi. Ushbu g'oyani xesh funksiyaga tadbiq etilsa, biror xabar va uning xesh qiymati berilganda xesh qiymatlari teng bo'lgan turli ma'lumotni topish masalasi qaraladi.

Biroq hujumchidan $N$ tug'ilgan kunlar orasida ixtiyoriy kolliziyani topish ehtimoli quyidagiga teng bo'ladi:

$$P_{kolliziya}(N) = 1 - \left(\frac{365}{365}\right)\left(\frac{364}{365}\right)\left(\frac{363}{365}\right)\cdots\left(\frac{365-N+1}{365}\right)$$

Ushbu holda ehtimollik ½ dan katta bo'lishi uchun $N=23$ imkoniyatning o'zi yetarli bo'ladi.

Agar hujumchi $n$ bitli xesh qiymat chiqaruvchi xesh funksiya uchun ½ dan ko'p bo'lgan ehtimollik bilan ixtiyoriy kolliziyani topishi $2^{n/2}$ ga teng bo'ladi.

Agar xesh funksiya uchun xesh qiymatning uzunligi $n$ bitga teng bo'lsa va u $p$ ehtimollik bilan aniqlanishi uchun kerak bo'lgan hisoblashlar soni $N$ ga teng bo'lsa, ular orasidagi bog'liqlikning mental ko'rinishi quyidagiga teng bo'ladi:

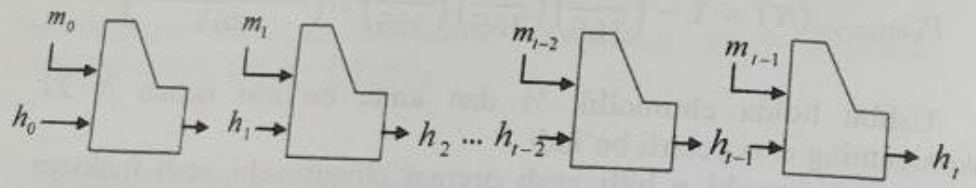
$$N \approx \sqrt{2 * 2^n * p}.$$

***Xesh funksiyalarni qurish usullari.*** Yuqorida keltirilgan siqish usullari asosida turli konstruksiyalardan foydalanilgan holda xesh funksiyalarni qurish amalga oshiriladi. Takroriy xeshlashga asoslangan funksiyalar hozirda keng tarqalgan usullardan biri bo'lib, xesh funksiyalarni qurishda keng foydalaniladi. Quyida keng tarqalgan xesh funksiyalarni qurish usullari keltirilgan.

*Merkle-Damgard (MD) usuli.* Ushbu usul xesh funksiyalarni qurishda eng keng tarqalgan usul sanalib, 1989-yilda R.Merkl va I.Damgard tomonidan ishlab chiqilgan. Ushbu usul odatda uchta qadamdan iborat bo'ladi. Birinchi qadamda ma'lumotga qo'shimcha ma'lumot qo'shish orqali uni teng bloklarga ajratish. Bunda keng tarqalgan to'ldirish usuli bu – bitta bir va qolganlarini nol bilan to'ldirishdir. Ikkinchi bosqich bu – kiritilgan ma'lumot bloki $m$ ni qism bloklarga $m_0, m_1, \dots, m_n$ ajratishdir. Shundan so'ng ochiq tanlab olingan boshlang'ich vektor va qism bloklardan foydalangan holda takroriy fiksirlangan qiymatlar hisoblanadi.

$$h_0 = IV,$$
$$h_i = f(h_{i-1}, m_{i-1})\ i = 1,2 \dots, t.$$

Bu yerda, $f$-siqish funksiyasi. Ushbu konstruksiyaning umumiy ko'rinish quyidagi 6.2 – rasmda keltirilgan.




*6.2 – rasm.* **Markle – Damgard konstruktori**

Sxemaning zaif tomonlari:

1. Ma'lumotni kerakli uzunlikkacha to'ldirish. Ya'ni, agar kriptoanalitik bitta kolliziya topsa, boshqalarini ham topish oson.
2. Xesh qiymatni beruvchi ikkinchi bir ma'lumotni (ikkinchi haqiqiyni) topish uzun ma'lumotlar uchun "to'liq tanlash hujumiga"ga nisbatan effektiv hisoblanadi.
3. Ma'lumotni to'ldirishga qaratilgan hujum, ya'ni, $X$ ma'lumotning xesh qiymati $H(X)$ ma'lum bo'lganida $H(pad(X)||Y)$ ning qiymatini topish oson bo'ladi. Bu yerda, $pad$-to'ldirish funksiyasi bo'lib, u $X$ga bog'liq bo'lgan ma'lumotning xesh qiymatini topish imkonini beradi.

*HAIFA usuli.* Merkle-Damgard usuli kolliziyaga bardoshli sanalib, yildan yil hisoblash qurilmalarining imkoniyatlari ortishi

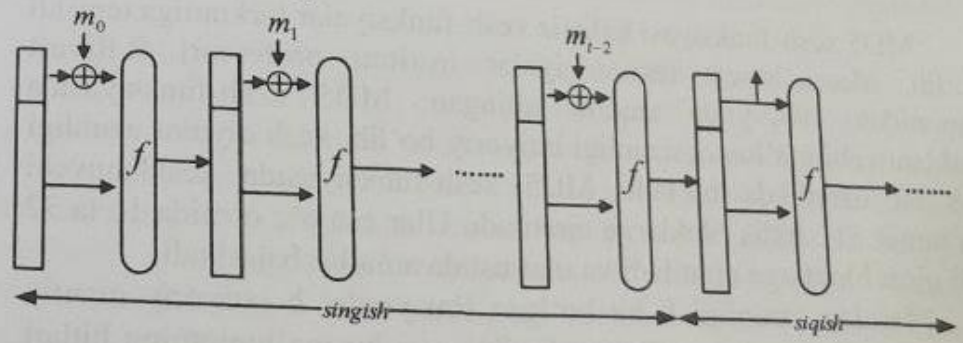


natijasida ko'plab hujumlarga zaif bo'lib bormoqda. Ushbu usuldagi kamchiliklar Biham va Dunkelmanlar tomonidan tuzatilib, yangi *HAIFA (HAsh Iterative FrAmework)* usulini taklif etilgan. HAIFA ham Merkle-Damgard usuli kabi takroriy sanalib, qo'shimcha ravishda xavfsizlikni oshirish uchun vosita kiritilgan.

MD usulida siqish funksiyasida kiruvchi qiymat sifatida $h_i$ va $m_i$ qiymatlar olinsa, HAIFAda esa ularga qo'shimcha ravishda $b$ va $s$ kattaliklar ham kiritiladi va umumiy ko'rinish quyidagicha bo'ladi: $h_i = f(h_{i-1}, m_{i-1}, b, s)$ ga teng bo'ladi.

*Sponge(gubka) usuli.* Ushbu funksiya xesh funksiya va oqimli shifrlarni yaratish uchun yangi usul sanalib, u tasodifiy almashtirish yoki tasodifiy funksiyaga asoslanadi. Agar $f$ funksiya tasodifiy almashtirish kabi tasvirlansa, unda $P$ – *sponge*, aks holda $T$ – *sponge* deb ataladi. Sponge usulida siqish va qolgan usullardagi siqish usullarining farqi, unda kirishdagi $l$ bit qiymat chiqishda ham $l$ bit shaklda ifodalanadi.

Ushbu usul ikkita bosqichdan iborat: *singish (absorbing)* va *siqish (squeezing)*. Birinchi bosqich takroriy holda bloklar ustida amalga oshiriladi. Bunda xabar bloki holat bilan takroriy holda XOR amalida qo'shiladi. Ushbu amal barcha bloklar ustida amalga oshirilgandan so'ng ikkinchi bosqich amalga oshiriladi. Bu bosqichda ba'zi qiymatlar chiqariladi va kutilgan xesh qiymat olingunga qadar $f$ funksiya qo'llaniladi (6.3-rasm).




*6.3 – rasm.* **Sponge konsturkutori**

Bulardan tashqari, xesh funksiyalarni qurishda *keng kanalli va ikki kanalli (Wide Pipe and Double Pipe), erkin old qo'shiluvchili Merkle-Damgard (Prefix-Free Merkle-Damgård), qobiqli Merkle-*

*Damgard (Enveloped Merkle-Damgård), RMX, 3C va 3C-X, dinamik xesh funksiya* konstruksiyalaridan keng foydalanilmoqda.

Xesh-funksiyalar ikki muhim turga, *kalitli* va *kalitsiz* xesh-funksiyalarga bo'linadi. Kalitli xesh-funksiyalar simmetrik kriptotizimlarda foydalaniladi. Ularni ma'lumotni autentifikatsiyalash kodlari deb ham atashadi. Ular bir-biriga ishonuvchi tomonlar uchun qo'shimcha vositalarsiz manbaning haqiqiyligi va ma'lumotning yaxlitligini kafolatlaydi. Kalitsiz xesh-funksiyalar xatolarni aniqlash kodlari deb ham yuritiladi. Kalitsiz xesh-funksiyalar qo'shimcha vositalarsiz ma'lumotning yaxlitligini kafolatlaydi. Bu xesh-funksiyalar bir-biriga ishonuvchi hamda bir-biriga ishonmaydigan tomonlar orasida ishlatiladi. Odatda kalitsiz xesh-funksiyalar quyidagi xossalarni qanoatlantirishi shart:

- bir tomonlamalik;
- kolliziyaga bardoshlilik;
- xesh qiymatlari teng bo'lgan ikkita ma'lumotni topishga bardoshlilik.

Keng foydalaniluvchi xesh-funksiyalar sifatida MD5, SHA1, SHA2, SHA3, GOST R 34.11-94, O'z DSt 1106 : 2006 algoritmlarini misol keltirish mumkin.

### 6.2. MD5 xesh funksiyasi

MD5 xesh-funksiyasi kalitsiz xesh-funksiyalar turkumiga tegishli bo'lib, Massachusets texnologiyalar instituti professori R.Rivest tomonidan 1992-yilda taqdim qilingan. MD5 xesh-funksiyasida xeshlanuvchi ma'lumot uzunligi ixtiyoriy bo'lib, xesh qiymat uzunligi 128 bit uzunlikda bo'ladi. MD5 xesh-funksiyasida xeshlanuvchi ma'lumot 512 bitlik bloklarga ajratiladi. Ular esa o'z o'rnida 16 ta 32 bitli qism bloklarga ajratiladi va ular ustida amallar bajariladi.

Masalan, uzunligi $b$ bit bo'lgan (bu yerda, $b$ ixtiyoriy manfiy bo'lmagan butun son) ma'lumot berilgan va bu ma'lumotning bitlari $m_0 m_1 \cdots m_{b-1}$ tartibda yozilgan. Xesh qiymatni hisoblash uchun quyidagi beshta bosqich bajariladi:

*1-bochqich.* To'ldirish bitlarini qo'shish.

Berilgan ma'lumot uzunligi $L$, 512 modul bo'yicha 448 bilan taqqoslanadigan ($L \equiv 448 \, mod \, 512$) ko'rinishda to'ldiriladi, ya'ni,



kengaytirilgan ma'lumotning uzunligi unga eng yaqin bo'lgan 512 ga karrali bo'lgan sondan 64 bitga kichik bo'lishi kerak. To'ldirish bosqichi, hamma vaqt xattoki ma'lumot uzunligi 512 modul bo'yicha 448 bilan taqqoslanadigan bo'lsa ham bajariladi. To'ldirish quyidagi tartibda amalga oshiriladi: ma'lumotga qiymati 1 ga teng bo'lgan bitta bit qo'shiladi, qolgan bitlar esa 0 lar bilan to'ldiriladi. Shuning uchun qo'shilgan bitlar soni 1 dan 512 tagacha bo'ladi.

Masalan, xabar $M$="message" ga teng bo'lsin. U holda xabarning ASCIIdagi ko'rinishi quyidagicha bo'ladi:

01101101 01100101 01110011 01110011 01100001 01100111 01100101

Xabar uzunligi $L = 56$ ga tengligi bois, qo'shiluvchi bitlar sonini 392 ga tengligini ko'rish mumkin: $(56 + 392) mod 512 = 448$. Shu sababli, birinchi bosqich natijasi quyidagicha bo'ladi:

01101101 01100101 01110011 01110011 01100001 01100111 01100101
*10000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*
*00000000 00000000 00000000 00000000 00000000 00000000 00000000*

*2-bosqich.* Ma'lumotning uzunligini qo'shish.

1-bosqichning natijasiga berilgan ma'lumot uzunligining 64 bitlik qiymati qo'shiladi. Agar ma'lumotning uzunligi $2^{64}$ bitdan katta bo'lsa, uzunlik $mod 2^{64}$ bo'yicha qo'shiladi. Shunday qilib, birinchi ikkita bosqich bajarilgandan keyin uzunligi 512 bitga karrali bo'lgan ma'lumot olinadi, ya'ni, kengaytirilgan ma'lumot uzunligi 16 ta 32 bitlik so'zdan iborat blok uzunligiga karrali bo'ladi. Natijada, hosil qilingan ma'lumot so'zlarini $M[0,\ldots,N-1]$ orqali belgilaymiz. U holda $N$ soni 16 ga karrali bo'ladi. Shunday qilib, $N = T \times 16$ bo'ladi.

Yuqoridagi misolda $L = 56$ bo'lgani bois, uning 64 bitli razryaddagi ko'rinishi quyidagicha bo'ladi:

*00000000 00000000 00000000 00000000 00000000 00000000 00000000 00111000*

*3-bosqich.* Xesh qiymat uchun bufer initsializatsiya qilish.

Xesh funksiyaning oraliq va oxirgi natijalarini saqlash uchun 128 bitli buferdan foydalaniladi. Bu buferni to'rtta 32 bitli $A$, $B$, $C$, $D$ registrlar ko'rinishida tasvirlash mumkin. Bu registrlarga 16 lik sanoq sistemasidagi quyidagi boshlang'ich qiymatlar beriladi:

$A = 0x01234567;$
$B = 0x89ABCDEF;$
$C = 0xFEDCBA98;$
$D = 0x76543210.$

*4-bosqich.* 512 bitli ma'lumotni 32 bitlik bloklarga ajratib qayta ishlash.

MD5 algoritmida argumenti va qiymati 32 bitli so'z bo'ladigan to'rtta funksiyadan foydalanilgan:

$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$
$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$
$H(X,Y,Z) = X \oplus Y \oplus Z$
$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$

Bu yerda, bitlar bo'yicha mantiqiy $AND$, $OR$, $NOT$, $XOR$ amallari mos ravishda $\wedge$, $\vee$, $\neg$, $\oplus$ belgilari bilan ifodalangan.

Shundan so'ng, 64 ta 32 bitli so'zdan iborat $K[0,\dots,63]$ massiv sinus funksiyasi asosida quyidagicha hosil qilinadi:

$$K[i] = [2^{32} \times abs(\sin(i))].$$

Bu yerda, $0 \le i \le 63$ ga teng. Ushbu tenglik natijasi quyida keltirilgan:

K[ 0.. 3] := {0xd76aa478, 0xe8c7b756, 0x242070db, 0xc1bdceee}
K[ 4.. 7] := {0xf57c0faf, 0x4787c62a, 0xa8304613, 0xfd469501}
K[ 8..11] := {0x698098d8, 0x8b44f7af, 0xffff5bb1, 0x895cd7be}
K[12..15] := {0x6b901122, 0xfd987193, 0xa679438e, 0x49b40821}



K[16..19] := {0xf61e2562, 0xc040b340, 0x265e5a51, 0xe9b6c7aa}
K[20..23] := {0xd62f105d, 0x02441453, 0xd8a1e681, 0xe7d3fbc8}
K[24..27] := {0x21e1cde6, 0xc33707d6, 0xf4d50d87, 0x455a14ed}
K[28..31] := {0xa9e3e905, 0xfcefa3f8, 0x676f02d9, 0x8d2a4c8a}
K[32..35] := {0xfffa3942, 0x8771f681, 0x6d9d6122, 0xfde5380c}
K[36..39] := {0xa4beea44, 0x4bdecfa9, 0xf6bb4b60, 0xbebfbc70}
K[40..43] := {0x289b7ec6, 0xeaa127fa, 0xd4ef3085, 0x04881d05}
K[44..47] := {0xd9d4d039, 0xe6db99e5, 0x1fa27cf8, 0xc4ac5665}
K[48..51] := {0xf4292244, 0x432aff97, 0xab9423a7, 0xfc93a039}
K[52..55] := {0x655b59c3, 0x8f0ccc92, 0xffeff47d, 0x85845dd1}
K[56..59] := {0x6fa87e4f, 0xfe2ce6e0, 0xa3014314, 0x4e0811a1}
K[60..63] := {0xf7537e82, 0xbd3af235, 0x2ad7d2bb, 0xeb86d391}

Bundan tashqari, 64 ta elementdan iborat $s$ massivdan foydalanilib, u siljitishlar sonini ifodalaydi:

s[ 0..15] :={7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22
}
s[16..31] :={5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20
}
s[32..47] :={4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23
}
s[48..63] :={6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21
}

MD5 xesh funksiyasida 64 raund davomida har bir 512 bitli blok ustida quyidagi amallar bajariladi:

*4.1.* 512 bitli blok $M$ 16 ta 32 bitli qismlarga ajratiladi: $M[j]$, $0 \le j \le 15$.

*4.2.* Quyidagilar o'zlashtiriladi:

$a = A;$
$b = B;$
$c = C;$
$d = D.$

*4.3.* 64 raund quyidagichasi bajariladi:

```
for i from 0 to 63 do:
    if 0≤i≤15 then:
        f=F(b,c,d);
```

```
        g=i;
    if 16≤i≤31 then:
        f=G(b,c,d);
        g=(5×i+1)mod16;
    if 32≤i≤47 then:
        f=H(b,c,d);
        g= (3×i+5) mod 16;
    if  48≤i≤63 then:
            f=I(b,c,d);
        g=(7×i)mod16;
        f=(f+a+K[i]+M[g])mod2^32;
    A=D;
    D=C;
    C=B;
    B=(B+leftrotate(f,s[i]))mod2^32;
    end for
    A=(A+a)mod2^32;
    B=(B+b)mod2^32;
    C=(C+c)mod2^32;
    D=(D+d)mod2^32.
```

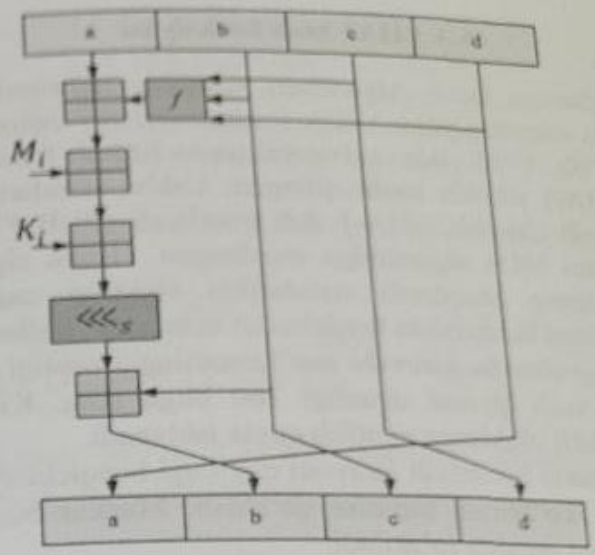
*4.4.* Barcha ma'lumot bloklari uchun 4.1 va 4.2-bosqichlar bajarilib bo'linganidan so'ng, yakuniy xesh qiymat quyidagicha hosil qilinadi:

$$h = A \parallel B \parallel C \parallel D.$$

Bu yerda, $\text{leftrotate}(x, c) = (x \ll c) \vee (x \gg (32 - c))$ ga teng.

Umumiy holda MD5 xesh funksiyasi bir raundining akslantirilishi 6.4-rasmda keltirilgan.






*6.4-rasm.* **MD5 algoritmining *t*-raundi**

MD5 funksiyasida kolliziya hodisasi aniqlangan bo'lib, quyida ushbu ikki bir-biridan farq qiluvchi ma'lumotlar keltirilgan.

$M_1$:
d131dd02c5e6eec4 693d9a0698aff95c 2fcab5[illegible]712467eab 4004583eb8fb7f89
55ad340609f4b302 83e4888325[illegible]1415a 085125e8f7cdc99f d91dbd[illegible]280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e2[illegible]487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080[illegible]80d1e c69821bcb6a88393 96f965[illegible]b6ff72a70

$M_2$:
d131dd02c5e6eec4 693d9a0698aff95c 2fcab5[illegible]712467eab 4004583eb8fb7f89
55ad340609f4b302 83e4888325[illegible]1415a 085125e8f7cdc99f d91dbd[illegible]280373c5b
d8823e3156348f5b ae6dacd436c919c6 dd53e2[illegible]487da03fd 02396306d248cda0
e99f33420f577ee8 ce54b67080[illegible]80d1e c69821bcb6a88393 96f965[illegible]b6ff72a70

Ushbu ikki ma'lumotning xesh qiymati "79054025255fb1a26e4bc422aef54eb4" ga teng. Shu sababli, yuqori darajadagi xavfsizlik talab etilgan tizimlarda ushbu algoritmdan foydalanish tavsiya etilmaydi.

## 6.3. SHA1 xesh funksiyasi

SHA (Secure Hash Algorithm) xeshlash algoritmi AQShning standartlar va texnologiyalar Milliy instituti (NIST) tomonidan ishlab chiqilgan bo'lib, 1992-yilda axborotni qayta ishlash federal standarti (PUB FIPS 180) sifatida nashr qilingan. Ushbu standart 1995-yilda qaytadan ko'rib chiqilib, SHA-1 deb nomlandi (PUB FIPS 180-1). SHA1 algoritmi MD4 algoritmiga asoslangan. Ushbu algoritm DSS (Digital Signature Standard) standartida elektron raqamli imzo algoritmlarini shakllantirishda foydalanish uchun mo'ljallangan.

SHA1 algoritmida kiruvchi ma'lumotning uzunligi $2^{64}$ bitdan kichik bo'lib, xesh qiymat uzunligi 160 bitga teng. Kiritilayotgan ma'lumot 512 bitli bloklarga ajratilib qayta ishlanadi.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

*1-bosqich.* To'ldirish bitlarini qo'shish. Mazkur bosqich MD5 algoritmidagi kabi amalga oshiriladi.

*2- bosqich.* Ma'lumotning uzunligini qo'shish. Ushbu bosqich ham MD5 algoritmida keltirilgani kabi amalga oshiriladi.

*3- bosqich.* Xesh qiymat uchun bufer initsializatsiya qilish.

SHA1 algoritmida oraliq va oxirgi natijalarini saqlash uchun 160 bitli buferdan foydalanilgan. Ushbu bufer beshta 32 bitli $A$, $B$, $C$, $D$, $E$ registrlardan tashkil topgan. Ushbu registorlarning 16 lik sanoq tizimidagi boshlang'ich qiymatlari quyida berilgan:

$A = 0x67452301;$
$B = 0xEFCDAB89;$
$C = 0x98BADCFE;$
$D = 0x10325476;$
$E = 0xC3D2E1F0.$

Keyinchalik ushbu o'zgaruvchilar mos ravishda yangi $a$, $b$, $c$, $d$ va $e$ o'zgaruvchilarga o'zlashtiriladi.

*4- bosqich.* Ma'lumotni 512 bitli bloklarga ajratib qayta ishlash.

SHA1 algoritmida har bir 512 bitli blok ustida 80 raund davomida qayta ishlash amalga oshiriladi. Ushbu algoritmda quyidagi o'zgarmaslar va funksiyalardan foydalanilgan:

Barcha raundlar uchun 32 bitli $K_t$ o'zgarmas qiymatlari:



$$K_t = \begin{cases} 0x5A827999, & 0 \le t \le 19 \\ 0x6ED9EBA1, & 20 \le t \le 39 \\ 0x8F1BBCDC, & 40 \le t \le 59 \\ 0xCA62C1D6, & 60 \le t \le 79 \end{cases}$$

$f_t(x,y,z)$ esa raundlar bo'yicha quyidagicha ifodalanadi:

$$f_t(x,y,z) = \begin{cases} (x \wedge y) \vee (\neg x \wedge z), & 0 \le t \le 19 \\ x \oplus y \oplus z, & 20 \le t \le 39, \quad 60 \le t \le 79 \\ (x \wedge y) \vee (x \wedge z) \vee (y \wedge z) & 40 \le t \le 59 \end{cases}$$

512 bitli blok ($M$) 16 ta 32 bitli qismlarga ajratiladi va undan 80 ta raund uchun $W_t$ quyidagicha hosil qilinadi:

$$W_t = \begin{cases} M_t, & 0 \le t \le 15 \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \lll 1, & 16 \le t \le 79 \end{cases}$$

SHA1 xesh funksiyasining asosiy sikli esa quyidagicha:

```
for t from 0 to 79 do:
```
$temp = ((a \lll 5) + f_t(b,c,d) + e + W_t + K_t) mod 2^{32};$
$e = d;\ \ d = c;\ \ c = b \lll 30;\ \ b = a;\ \ a = temp;$
```
end for
```

Asosiy sikl tugagandan keyin $a$, $b$, $c$, $d$ va $e$ larning qiymatlari mos ravishda $A$, $B$, $C$, $D$ va $E$ registrlardagi qiymatlariga qo'shiladi va ma'lumotning keyingi 512 bitli blokini qayta ishlashga o'tiladi.

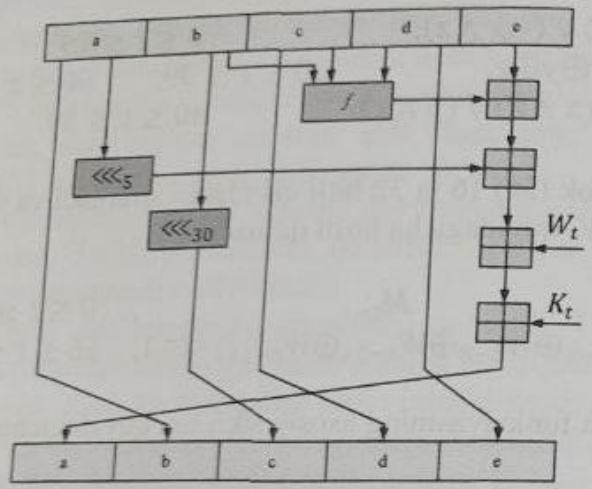
$A = (A+a) \bmod 2^{32};$
$B = (B+b) \bmod 2^{32};$
$C = (C+c) \bmod 2^{32};$
$D = (D+d) \bmod 2^{32};$
$E = (E+e) \bmod 2^{32}.$

*5- bosqich.* Yakuniy xesh qiymatni hosil qilish.

Ma'lumotning xesh qiymati $A$, $B$, $C$, $D$ va $E$ registrlardagi qiymatlarni birlashtirish natijasida hosil qilinadi:

$$h = A \parallel B \parallel C \parallel D \parallel E.$$

6.5-rasmda SHA1 xesh funksiyasi algoritmining $i$-raund ko'rinishi keltirilgan.




*6.5-rasm.* **SHA1 algoritmining *i*-raundi**

MD5 algoritmi kabi, SHA1 algoritmi uchun ham kolliziya holati aniqlangan. 2017-yilda Google tashkiloti va CWI (Centrum Wiskunde & Informatica) markazi mutaxassislari tomonidan bir xil xesh qiymatni beruvchi ikkita turli PDF formatidagi fayllar generatsiya qilingan.

### 6.4. O'z DSt 1106 : 2006 xesh funksiyasi

Ushbu standart ikkita algoritmdan iborat ular 1-algoritm va 2-algoritm deb nomlangan. 1-algoritmda kirish ketma-ketligining uzunligi 128 yoki 256 bitga karrali bo'lib, chiqish ketma-ketligi va xeshlash kaliti qayd etilgan 128 yoki 256 bit uzunlikka ega.

Birinchi algoritm parametrli algebga muammosiga asoslangan bo'lsa, ikkinchi algoritm ГОСТ 28147-89 blokli shifrlash algoritmiga



asoslangan. Ushbu standartda quyidagi belgilanishlar va sozlanmalar mavjud:

*O'z DSt 1106:2009 – birinchi algoritm.* Ushbu algoritmning tavsifi quyida keltirilgan. Birinchi algoritm uchun quyidagi belgilanishlar qabul qilingan:

$M$ - dastlabki ma'lumot (xabar);

$h$ – xesh funksiya;

$m$ – xesh funksiya qiymati, bunda $m = h(M)$;

$k$ - xeshlash kaliti;

$k_e$ - *4x8* tartibli ikki o'lchamli massiv ko'rinishidagi bosqich kaliti;

*holat* - *4x8* tartibli ikki o'lchamli massiv ko'rinishidagi xeshlashning oraliq natijasi;

*holatn* - *4x8* tartibli ikki o'lchamli massiv ko'rinishidagi kirish bloki;

$r$ - modul, bunda $p \in \{16, 256\}$;

$e$ - xeshlash protsedurasining bosqichlar soni;

$b$ - dastlabki ma'lumotlardagi bloklar soni;

$\oplus$ - *XOR* amalining simvoli (2-modul bo'yicha qo'shish amallari);

$\otimes$ - diamatritsalarni $r$ moduli bo'yicha ko'paytirish amalining simvoli;

® - parametr bilan $r$ moduli bo'yicha ko'paytirish amalining simvoli;

$^{-1}$ - $r$ moduli bo'yicha teskarilash amalining simvoli;

$\backslash^{-1}$ – parametr bilan $r$ moduli bo'yicha teskarilash amalining simvoli;

$\backslash^{x}$ - parametr bilan $r$ moduli bo'yicha $x$ darajaga ko'tarish amalining simvoli;

XF - xeshlash funksiyasi;

NY - nazorat summasi;

|| - konkatenatsiya simvoli.

XFda quyidagi parametr va funksiyalar foydalaniladi:

a) $k$ – yarim bayt (bayt) darajasidagi chiziqli massivi ko'rinishidagi *128* yoki *256* bit uzunlikdagi xeshlash kaliti;

b) $k_e$ - *4x8* tartibdagi ikki o'lchamli massiv ko'rinishidagi bosqich (raund) kaliti;

c) *b* – dastlabki ma'lumotlardagi bloklar soni;

d) *uzunlik* – dastlabki ma'lumotlarning bitlardagi uzunligini o'z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma'lumotlarning oxirgidan oldingi bloki;

e) *NY* - o'nlik sanoq tizimida dastlabki ma'lumotlar qiymatlari summasini o'z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma'lumotlarning oxirgi bloki;

f) *r* - modul, $r \in \{16,256\}$;

g) $e_0$ - *128* va *(256)* bitli kirish bloklari uchun *(b +2)10* ga teng bo'lgan xeshlash protsedurasi bosqichlarining umumiy soni;

h) *Qo'sh (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida *p* moduli bo'yicha *(A, B, R)* parametri bilan darajaga ko'tarish amali asosida xeshlash protsedurasida foydalaniladigan o'zgartirish;

i) *BaytZichlash (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida, agar modul *p=16* bo'lsa, *XOR* amalidan foydalanilgan holda yoki agar modul *p=256* bo'lsa, bitta massivga zichlash chiziqli massivi asosida xeshlash protsedurasida foydalaniladigan o'zgartirish;

j) *Aralash(holat, $k_e$)* – diamatritsalarni ko'paytirish amali asosida xeshlash protsedurasida foydalaniladigan o'zgartirish. Bu yerda ko'paytiriladigan diamatritsalar, mos ravishda, *holat* va $k_e$ bosqich kaliti ikki o'lchamli massivlarining kvadrat shaklidagi chap va o'ng yarimlariga o'zaro mos keladi;

k) *SurHolat(holat)* - *holat* massivi ustida amalga oshiriladigan, xeshlash protsedurasida foydalaniladigan o'zgartirish, bu *holat* massivining barcha to'rtta satrini gorizontal va vertikal bo'yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

l) *SurKalit($k_e$)* - $k_e$ massivi ustida amalga oshiriladigan xeshlash protsedurasida foydalaniladigan o'zgartirish, bu $k_e$ massivining barcha to'rtta satrini gorizontal va vertikal bo'yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

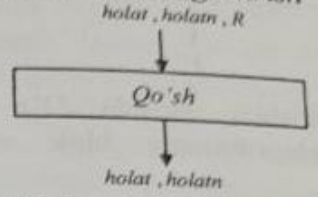
m) *TuzilmaKalit($k_e$, k)* - xeshlash protsedurasining har bir bosqichi so'ngida foydalaniladigan o'zgartirish, bu uning strukturasini dastlabki xeshlash kaliti *k* strukturasiga keltirish maqsadida $k_e$ massivining har bir yarim bayti (bayti) ustida amalga oshiriladi; ushbu o'zgartirish natijasi $k_e$ massivining kvadrat qismlaridan har birini



teskarilash shartlarini qanoatlantiradi.

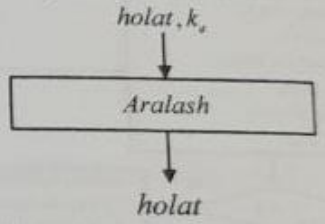
Keltirilgan almashtirishlarning umumiy ko'rinishi quyidagicha:

1. *Qo'sh(holat, holatn, R) o'zgartirish*

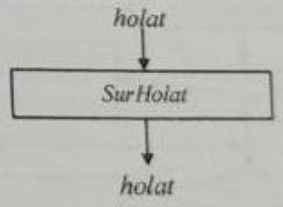



2. *BaytZichlash(holat, holatn)* o'zgartirishi

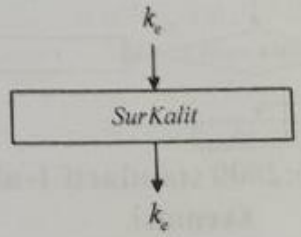

3. *Aralash(holat, $k_e$) o'zgartirishi*



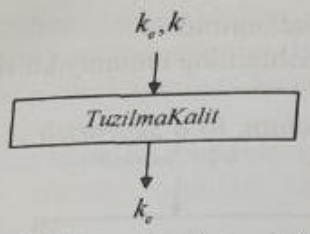

4. *SurHolat(holat) o'zgartirishi*



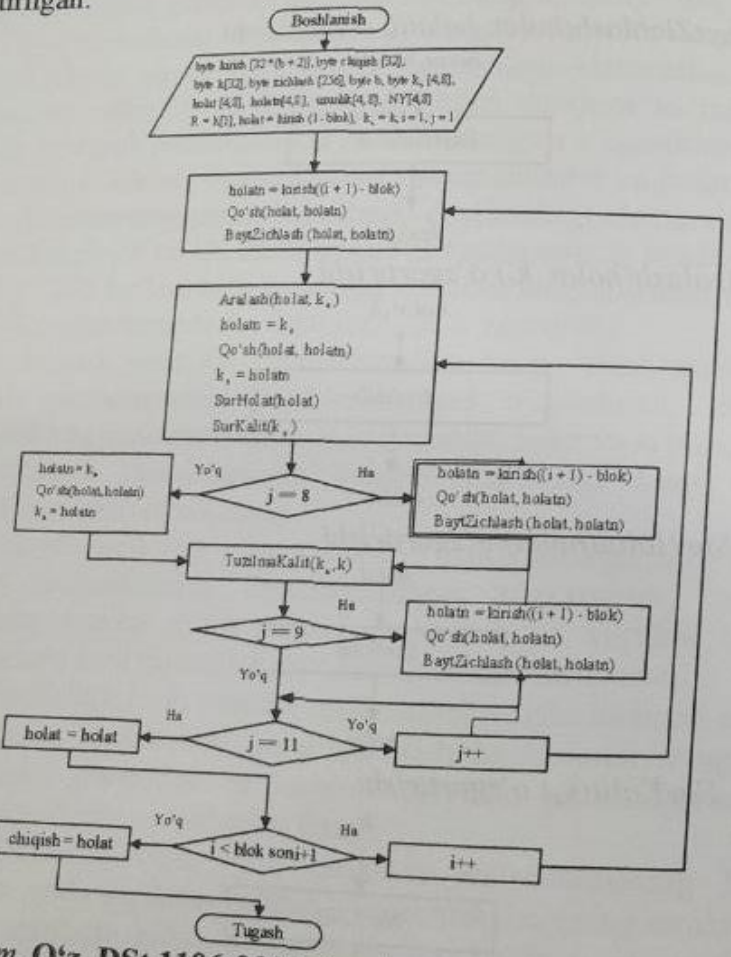

5. *SurKalit($k_e$) o'zgartirishi*




6. *TuzilmaKalit($k_e$,k) o'zgartirishi*




Keltirilgan akslantirishlar asosida O‘z DSt 1106:2009 standartining birinchi algoritmining blok sxemasi 6.6-rasmda keltirilgan.

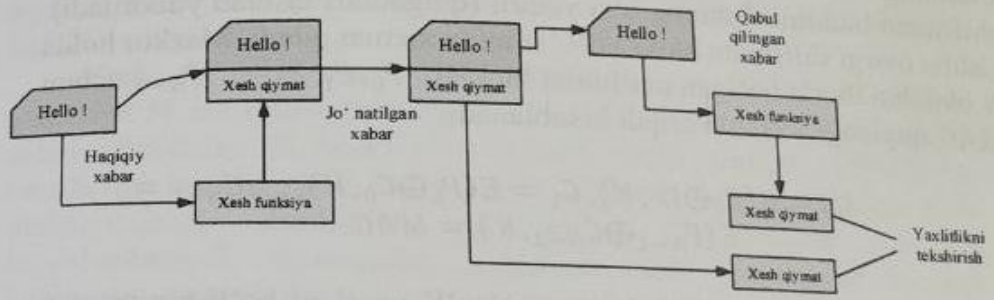



*6.6-rasm.* **O‘z DSt 1106:2009 standarti 1-algoritmining blok-sxemasi**



## 6.5. Ma’lumotlarni autentifikatsiyalash kodlari. HMAC algoritmi

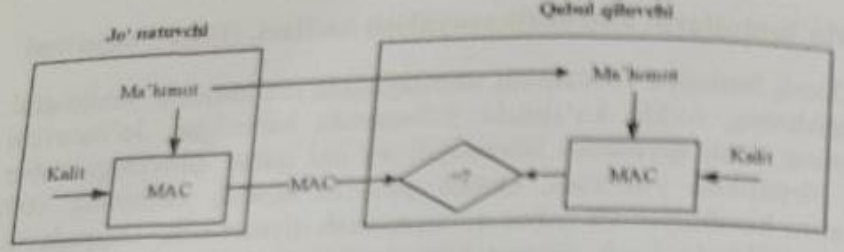
Xesh funksiya yordamida uzatilayotgan ma’lumotlar yaxlitligini tekshirishning sodda ko‘rinishi 6.7-rasmda keltirilgan. Jo‘natuvchi xabarning xesh qiymatini hisoblaydi va uni qabul qiluvchiga xabar bilan birgalikda yuboradi. Qabul qiluvchi dastlab xabarning xesh qiymatini hisoblaydi va qabul qilingan xesh qiymat bilan taqqoslaydi. Agar har ikkala xesh qiymat teng bo‘lsa, ma’lumotning yaxlitligi o‘zgarmagan, aks holda o‘zgargan deb topiladi. Odatda xesh funksiya kirishda ma’lumotdan tashqari hech qanday qiymatni talab etmagani bois, *kalitsiz kriptografik funksiyalar* deb ham ataladi (kalit talab qiluvchi ma’lumotlarning yaxlitligini ta’minlash usullari ham mavjud).




*6.7-rasm.* **Xesh funksiya asosida ma’lumotlar yaxlitligini tekshirish**

Yuqorida keltirilgan usulda xavfsizlik muammosi jiddiy bo‘lgani bois, undan amalda foydalanilmaydi. Ya’ni, hujumchi tomonidan faqat ma’lumot o‘zgartirilgan holda yaxlitlikni tekshirish imkoniyati mavjud. Biroq, hujumchi ma’lumotning xesh qiymatini almashtirish orqali foydalanuvchini osonlik bilan ma’lumot yaxlitligiga ishontirishi mumkin. Buning asosiy sababi, ma’lumotning xesh qiymatini hosil qilishda hujumchiga noma’lum biror axborotdan foydalanilmaganligi.

Ushbu muammoni bartaraf etuvchi – *xabarlarni autentifikatsiyalash kodi (message authentication code, MAC)* tizimlari mavjud bo‘lib, unga ko‘ra biror maxfiy kalit asosida ma’lumotning xesh qiymati hisoblanadi (6.8-rasm).




*6.8-rasm.* **MAC tizimi**

MAC tizimlarini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC (Cipher Block Chaining – shifr bloklar zanjiri) rejimida foydalanish va eng oxirgi shifrmatn blokini olishning o'zi yetarli (qolganlari tashlab yuboriladi). Ushbu oxirgi shifrmatn bloki *MAC* sifatida xizmat qiladi. Mazkur holda $N$ blokdan iborat bo'lgan ma'lumot bloklari, $P_0, P_1, P_2, \dots, P_{N-1}$ uchun MAC quyidagi formula orqali hisoblanadi:

$$C_0 = E(P_0 \oplus IV, K), C_1 = E(P_1 \oplus C_0, K), \dots, C_{N-1} = E(P_{N-1} \oplus C_{N-2}, K) = MAC.$$

Buning uchun har ikkala tomonda $IV$ va $K$ ni bo'lishining o'zi yetarli.

Faraz qilaylik, A va B tomonlardan uzatilayotgan ma'lumotlar yaxlitligini tekshirish talab etilgan bo'lsin (bu yerda ma'lumot konfidensialligini ta'minlash masalasi qaralmagan). Bu holda A va B tomonlar orasida xavfsiz taqsimlangan $K$ kalit yordamida A tomon $MAC$ ni hisoblaydi va ma'lumotni $IV$ ga qo'shib B ga uzatadi. B tomon ma'lumot, $K$ va $IV$ yordamida $MAC$ ni hisoblaydi. Agar hisoblangan $MAC$ qabul qilingan $MAC'$ ga teng bo'lsa, ma'lumot o'zgartirilmagan aks holda o'zgartirilgan deb topiladi.

Qanday qilib, ikkita hisoblangan $MAC$ qiymatlar turlicha bo'lishi mumkin? Faraz qilaylik, A tomon quyidagilarni B ga yuborgan bo'lsin:

$$IV, P_0, P_1, P_2, P_3, MAC.$$



Faraz qilaylik, hujumchi birinchi blok $P_1$ ni o'zgartirdi (u $Q$ deb belgilansin), bu holda B tomon MAC ni quyidagicha hisoblaydi: $C_0 = E(P_0 \oplus IV, K), \hat{C}_1 = E(Q \oplus C_0, K), \hat{C}_2 = E(P_2 \oplus \hat{C}_1, K), \hat{C}_3 = E(P_3 \oplus \hat{C}_2, K) = "MAC" \neq MAC$.

Ya'ni, ochiq matndagi bir blokning o'zgarishi keyingi barcha bloklarga ta'sir qiladi va buning natijasida shifrmatn bloklari turlicha bo'ladi. Ma'lumki, CBC rejimida shifrmatndagi bir blok o'zgarishi rasshifrovkalanganda faqat 2 ta ochiq matn blokiga ta'sir qiladi. Biroq, ochiq matnning bir blokini o'zgarishi undan keyingi barcha shifrmatn bloklariga ta'sir qiladi va bu MAC tizimlari uchun juda muhim.

Albatta, mazkur usul MAC tizimlarini yaratishning yagona usuli emas. Quyida xesh funsiyalar asosida MAC tizimlarini yaratish bilan tanishib chiqiladi.

***Xesh – funksiyalar asosida ma'lumot yaxlitligini tekshirish.*** Yuqorida $M$ ma'lumot yaxlitligini tekshirishda $h(M)$ ni hisoblash va qabul qiluvchiga $M, h(M)$ ni yuborish orqali amalga oshirishning kamchiligi haqida aytib o'tilgan edi. Shuning uchun, amalda xesh funksiyalardan ma'lumot yaxlitligini ta'minlashda bevosita foydalanilmaydi. Boshqacha aytganda, xesh funksiyalar asosida ma'lumot yaxlitligini ta'minlashda hisoblangan xesh qiymatni o'zgartira olmaslikni kafolatlash zarur. Buni amalga oshirish uchun balki xesh qiymatni simmetrik kalitli shifrlar asosida shifrlash zarurdir (ya'ni, $E(h(M), K)$). Biroq, buni amalga oshirishning soddaroq usuli – *xeshlangan MAC* (hashed MAC yoki HMAC) usuli mavjud. Bu usulga ko'ra, xesh qiymatni shifrlashning o'rniga, xesh qiymatni hisoblash jarayonida kalitni bevosita ma'lumotga biriktirish amalga oshiriladi. HMAC tizimida kalitlar qanday biriktiriladi? Umumiy holda ikki usul: kalitni matnni oldidan qo'yish ($h(K, M)$) yoki kalitni matndan keyin qo'yish ($h(M, K)$) mavjud bo'lsada, ularning har ikkalasida jiddiy xavfsizlik muammosi mavjud.

Xesh funksiyalar ham simmetrik kriptotizim hisoblanadi va simmetrik blokli shifrlash kabi ma'lumotlarni xeshlashda bloklarga ajratiladi. Odatda aksariyat xesh funksiyalar uchun (masalan, MD5, SHA1, Tiger) blok uzunligi 64 baytga yoki 512 bitga teng.

*HMAC* tizimida kalit ma'lumotga quyidagicha biriktiriladi. Dastlab xesh funksiyadagi blokning uzunligi baytlarda aniqlanadi

Masalan. MD5 xesh funksiyasida blok uzunligi $B = 64$ baytga teng bo'lsin. Olingan kalit $(K)$ uzunligi ham blok uzunligiga keltiriladi. Bunda 3 ta holat bo'lishi mumkin: (1) agar kalitning uzunligi 64 baytga teng bo'lsa, hech qanday o'zgarish amalga oshirilmaydi, (2) agar kalitning uzunligi 64 dan kichik bo'lsa, u holda yetmagan baytlar o'rni nollar bilan to'ldiriladi, (3) agar kalit uzunligi blok uzunligidan katta bo'lsa, kalit dastlab xeshlanadi va hosil bo'lgan xesh qiymatning o'ng tomoni blok uzunligiga yetguncha nollar bilan to'ldiriladi. Shu tariqa, kalit uzunligi blok uzunligiga moslashtiriladi.

Shunday qilib, ma'lumot va moslashtirilgan kalit asosida HMAC qiymati quyidagicha hisoblanadi:

$$HMAC(M,K) = H\big(K \oplus opad, H(K \oplus ipad, M)\big).$$

Bu yerda, $ipad$ va $opad$ o'zgaruvchilar quyidagicha hosil qilinadi:

$$ipad = 0x36 \text{ ni } B \text{ marta takrorlash natijasida}$$
$$opad = 0x5c \text{ ni } B \text{ marta takrorlash natijasida}$$

Tenglikdan ko'rinib turibdiki, HMAC da ikki marta xeshlash amalga oshirilmoqda. Kalit $K$ faqat ikki tomonga (jo'natuvchi va qabul qiluvchiga) ma'lum bo'lgani uchun, hujumchi mos xesh qiymatni qayta hisoblay olmaydi. A tomondan yuborilgan $(M, HMAC(M,K))$ ma'lumot juftlaridan hujumchi faqat ma'lumotni o'zgartirishi mumkin bo'ladi va bu holat qabul qiluvchi tomonidan osonlik bilan aniqlanadi.

***GCM (Galois/Counter Mode) rejimi.*** GCM – simmetrik blokli shifrlash algoritmlari uchun amalga oshirish rejimi bo'lib, yuqori samaradorligi bois keng qo'llaniladi. Ushbu rejim ham konfidensiallik, ham yaxlitlikni ta'minlash maqsadida ishlab chiqilgan bo'lib, 128 bitli blok uzunligidagi blokli shifrlar uchun mo'ljallangan.

GCM rejimida ikkita amal: autentifikatsiyalangan shifrlash va autentifikatsiyalangan rasshifrovkalash, mavjud. Autentifikatsiyalangan shifrlash amali uchun 4 ta kirish parametrli bo'lib, ular quyidagilar:

- maxfiy kalit $K$ – tanlangan blokli shifrlash algoritmining kaliti;



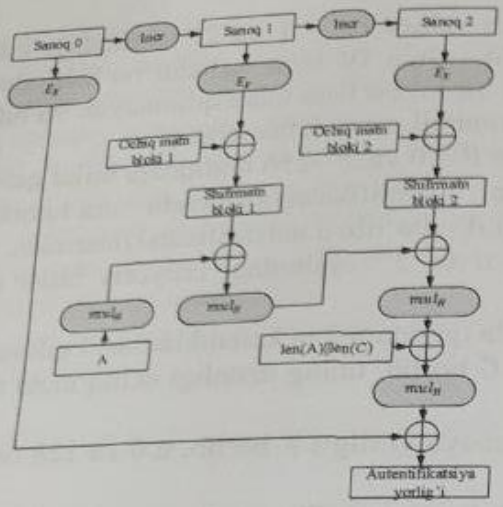
- boshlang'ich vektor $IV$ – 1 va $2^{64}$ oraliqdagi ixtiyoriy bitlar qatori. Har bir kalit uchun IV ham turlicha bo'lishi shart va bunda ularning uzunligini bir xil bo'lishi talab qilinmaydi. 96 bitli IV amalga oshirishdagi eng samarali uzunlik hisoblanadi;
- ochiq matn $P$ – 0 va $2^{39}$-256 oraliqdagi bitlar qatori;
- qo'shimcha autentifikatsiyalanuvchi ma'lumot (Additional authenticated data) $A$ – bo'lib, u autentifikatsiyalansada, shifrlanmaydi va ushbu kattalik 0 va $2^{64}$ oraliqdagi ixtiyoriy bitlar qatori bo'lishi mumkin;

GCM amalida quyidagi 2 ta kattaliklar hosil qilinadi:

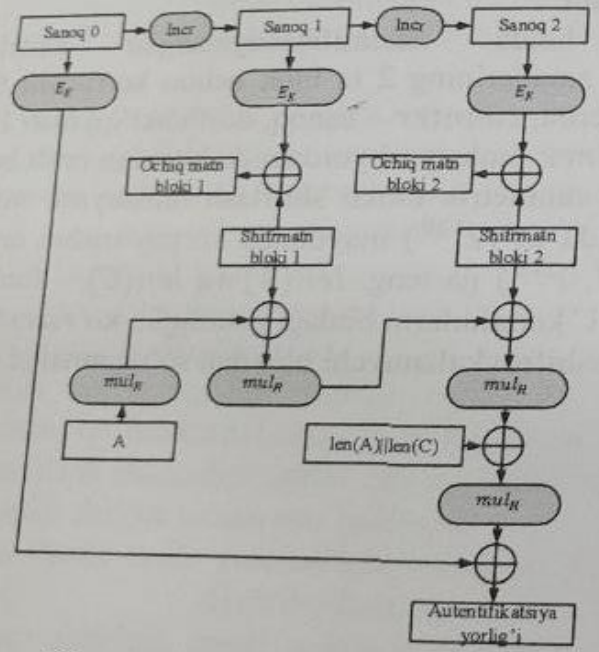
- shifrmatn $C$ bo'lib, uning uzunligi ochiq matn uzunligiga teng bo'ladi;
- autentifikatsiya yorlig'i $T$ bo'lib, u 0 va 128 oralig'idagi bitlar qatoridir.

GCM rejimining autentifikatsiyalangan rasshifrovkalash amalida esa $K, IV, C, A$ va $T$ parametrlari kiritiladi hamda chiqishda ochiq matn $P$ yoki autentikatsiyadan o'ta olmaganlik holatini ko'rsatuvchi $FAIL$ belgisi hosil bo'ladi.

Umumiy holda autentifikatsiyalangan shifrlash va rasshifrovkalash amallarining 2 ta blok uchun ko'rinishi 6.9-rasmda keltirilgan. Bu yerda, $counter$ – sanoq, dastlabki qiymati IV va u har bir blok uchun $incr$ funksiyasi yordamida bittadan ortib boradi. $E_K$ – kalit yordamida simmetrik blokli shifrlash funksiyasi, $mul_H$ – xesh kalit $H$ yordamida $GF(2^{128})$ maydonda ko'paytirishni anglatadi. Bu yerda, $H = E(K, 0^{128})$ ga teng. $len(A)$ va $len(C)$ – funksiyalar esa mos holda A va C kattaliklarni bitdagi uzunligini ko'rsatadi va u oxirgi shiflanuvchi/ rasshifrovkalanuvchi blokdan so'ng amalga oshiriladi.




a) Autentifikatsiyalangan shifrlash amali




b) Autentifikatsiyalangan rasshifrovkalash amali

*6.9-rasm.* **GCM rejimi**



GCM rejimida ko'plab standartlarda, IEEE 802.1AE, IEEE 802.11ad, ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1, IETF Ipsec, SSH, TLS 1.2 va 1.3, qo'llanilgan.

**Nazorat savollari**

1. Xesh funksiyaga ta'rif bering.
2. Xesh funksiyalarga qo'yilgan talablarni ayting.
3. Xesh funksiyalarni qurish usullari haqida ayting.
4. Xesh funksiyada kolliziya hodisasi nima?
5. MD5 xesh funksiyasi va uning matematik asosi haqida ayting.
6. MD5 xesh funksiyasiga ma'lumotga to'ldirish bitlari qanday qo'shiladi.
7. SHA1 xesh funksiyasi va uning matematik asosi haqida gapiring.
8. O'z DSt 1106 : 2006 xesh funksiyasi va uning matematik asosi haqida ayting.
9. Xabarlarni autentifikatsiyalash kodi nima va uning asosiy vazifasini tushuntiring.
10. MAC tizimlarida kalitdan foydalanishdan asosiy maqsadni tushuntiring.
11. HMAC algoritmining ishlash tartibini tushuntiring.
12. GCM rejimi va uning asosiy vazifasini ayting.

## FOYDALANILGAN ADABIYOTLAR


1. A.J.Menezes, P.C. van Oorschot, S.A.Vanstone. Handbook of Applied Cryptography. CRC Press, 2001, 816 p.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 -816 стр.

3. С.К.Ганиев, М.М.Каримов, З.Т.Худойкулов, М.М.Кадиров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках. –Т.: «Иктисод-молия», - 2017, 480 с.

4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.

5. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.

6. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.

7. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –T.: «Iqtisod-moliya», - 2021, 228 bet.

8. D.Ya.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.

9. Akbarov D.Ye. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, -B. - 394.

10. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии: Учебное пособие, 2-е изд. – М.: Гелиос АРВ, 2002.-480 с.

11. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. –Toshkent, 2008. - 208 bet.

12. O‘z DSt 1105:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.

13. O‘z DSt 1106:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi.

14. David A. McGrew, John Viega. The Galois/Counter Mode of Operation (GCM), 2001. https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf

15. DES Modes of Operation. Federal Information Processing Standards Publication 81, December, 1980.

16. Federal Information, Processing Standards Publication 197. Announcing the Advanced Encryption Standard (AES). November 26, 2001.

17. Rogaway, P., Coppersmith, D. A Software-Optimized Encryption Algorithm. J.Cryptology 11, 273–287 (1998). https://doi.org/10.1007/s001459900048


### Internet resurslari


1. Twofish: A 128-Bit Block Cipher [sayt]: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf (murojaat vaqti: 26.04.2024).

2. MD5 [sayt]: https://en.wikipedia.org/wiki/MD5 (murojaat vaqti: 26.04.2024).

3. SHA-1 [sayt]: https://en.wikipedia.org/wiki/SHA-1 (murojaat vaqti: 26.04.2024).

4. HMAC [sayt]: https://en.wikipedia.org/wiki/HMAC (murojaat vaqti: 26.04.2024).

5. International Data Encryption Algorithm [sayt]: https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm (murojaat vaqti: 26.04.2024).

6. GOST 28147-89 [sayt]: https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89 (murojaat vaqti: 26.04.2024).

7. A5/1 [sayt]: https://en.wikipedia.org/wiki/A5/1 (murojaat vaqti: 26.04.2024).

8. RC4 [sayt]: https://en.wikipedia.org/wiki/RC4 (murojaat vaqti: 26.04.2024).

9. Enigma Machine Emulator [sayt]: https://www.101computing.net/enigma-machine-emulator/ (murojaat vaqti: 26.04.2024).

10. WAKE [sayt]: https://ru.wikipedia.org/wiki/WAKE (murojaat vaqti: 26.04.2024).

1-ilova

128 bitli AES kalitini kengaytirish

$K = 2b\ 7e\ 15\ 16\ 28\ ae\ d2\ a6\ ab\ f7\ 15\ 88\ 09\ cf\ 4f\ 3c$

$N_k = 4$ bo'lgani bois quyidagi o'rinli:

$w_0 = 2b\ 7e\ 15\ 16$, $w_1 = 28\ ae\ d2\ a6$, $w_2 = ab\ f7\ 15\ 88$, $w_3 = 09\ cf\ 4f\ 3c$.

| i (dec) | Temp | RotWord() dan s'ong | SubWord() dan s'ong | Rcon[i/Nk] | Rcon bilan XOR amalidan s'ong | w[i-Nk] | w[i]=temp XOR w[i-Nk] |
|---|---|---|---|---|---|---|---|
| 4 | 09cf4f3c | cf4f3c09 | 8a84eb01 | 01000000 | 8b84eb01 | 2b7e1516 | a0fafe17 |
| 5 | a0fafe17 | | | | | 28aed2a6 | 88542cb1 |
| 6 | 88542cb1 | | | | | abf71588 | 23a33939 |
| 7 | 23a33939 | | | | | 09cf4f3c | 2a6c7605 |
| 8 | 2a6c7605 | 6c76052a | 50386be5 | 02000000 | 52386be5 | a0fafe17 | f2c295f2 |
| 9 | f2c295f2 | | | | | 88542cb1 | 7a96b943 |
| 10 | 7a96b943 | | | | | 23a33939 | 5935807a |
| 11 | 5935807a | | | | | 2a6c7605 | 7359f67f |
| 12 | 7359f67f | 59f67f73 | cb42d28f | 04000000 | cf42d28f | f2c295f2 | 3d80477d |
| 13 | 3d80477d | | | | | 7a96b943 | 4716fe3e |
| 14 | 4716fe3e | | | | | 5935807a | 1e237e44 |
| 15 | 1e237e44 | | | | | 7359f67f | 6d7a883b |
| 16 | 6d7a883b | 7a883b6d | dac4e23c | 08000000 | d2c4e23c | 3d80477d | ef44a541 |
| 17 | ef44a541 | | | | | 4716fe3e | a8525b7f |
| 18 | a8525b7f | | | | | 1e237e44 | b671253b |
| 19 | b671253b | | | | | 6d7a883b | db0bad00 |
| 20 | db0bad00 | 0bad00db | 2b9563b9 | 10000000 | 3b9563b9 | ef44a541 | d4d1c6f8 |
| 21 | d4d1c6f8 | | | | | a8525b7f | 7c839d87 |
| 22 | 7c839d87 | | | | | b671253b | caf2b8bc |
| 23 | caf2b8bc | | | | | db0bad00 | 11f915bc |
| 24 | 11f915bc | f915bc11 | 99596582 | 20000000 | b9596582 | d4d1c6f8 | 6d88a37a |
| 25 | 6d88a37a | | | | | 7c839d87 | 110b3efd |
| 26 | 110b3efd | | | | | caf2b8bc | dbf98641 |
| 27 | dbf98641 | | | | | 11f915bc | ca0093fd |
| 28 | ca0093fd | 0093fdca | 63dc5474 | 40000000 | 23dc5474 | 6d88a37a | 4e54f70e |
| 29 | 4e54f70e | | | | | 110b3efd | 5f5fc9f3 |
| 30 | 5f5fc9f3 | | | | | dbf98641 | 84a64fb2 |
| 31 | 84a64fb2 | | | | | ca0093fd | 4ea6dc4f |
| 32 | 4ea6dc4f | a6dc4f4e | 2486842f | 80000000 | a486842f | 4e54f70e | ead27321 |
| 33 | ead27321 | | | | | 5f5fc9f3 | b58dbad2 |
| 34 | b58dbad2 | | | | | 84a64fb2 | 312bf560 |
| 35 | 312bf560 | | | | | 4ea6dc4f | 7f8d292f |
| 36 | 7f8d292f | 8d292f7f | 5da515d2 | 1b000000 | 46a515d2 | ead27321 | ac7766f3 |
| 37 | ac7766f3 | | | | | b58dbad2 | 19fadc21 |
| 38 | 19fadc21 | | | | | 312bf560 | 28d12941 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 39 | 28d12941 | | | | | 7f8d292f | 575c006e |
| 40 | 575c006e | 5c006e57 | 4a639f5b | 36000000 | 7c639f5b | ac7766f3 | d014f9a8 |
| 41 | d014f9a8 | | | | | 19fadc21 | c9ee2589 |
| 42 | c9ee2589 | | | | | 28d12941 | e13f0cc8 |
| 43 | e13f0cc8 | | | | | 575c006e | b6630ca6 |



## ATAMALARNING RUS, O'ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG'ATI

**Алгоритм** - упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

**Algoritm** – amallarning cheklangan soni yordamida masala yechimini belgilovchi buyruqlarning cheklangan to'plami.

**Algorithm** - an ordered finite set of clearly defined rules for solving problems in a finite number of steps.

**Алгоритм Rijndael** - криптографический алгоритм, указанный в Advanced Encryption Standard.

**Rijndael algoritmi** - Advanced Encryption Standardda ko'rsatilgan kriptografik algoritm.

**Rijndael** – cryptographic algorithm specified in the Advanced Encryption Standard.

**Алгоритм SHA** - хэш-алгоритм со свойствами, которые в вычислительном отношение неосуществимы: 1) чтобы найти сообщение, которое соответствует данному дайджесту сообщения или 2) найти два различных сообщения, которые производят тот же самый дайджест сообщения.

**SHA algoritmi** - 1) berilgan xabar daydjestiga mos xabarni topish yoki 2) bir xil xabar daydjestini hosil qiluvchi ikkita turli xabarlarni hisoblash orqali topish imkonsiz bo'lgan xususiyatlarga ega xesh - algoritm.

**Secure hash algorithm (SHA)** – a hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

**Алгоритм шифрования блочный базовый** - алгоритм шифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков текста открытого, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины.

**Shifrlashning bazaviy blokli algoritmi** - kalitning har bir muayyan qiymatida belgilangan uzunlikdagi ochiq matn bloklari to'plami ustida bitta qaytariluvchi akslantirishni amalga oshiruvchi shifrlash algoritmi. Belgilangan uzunlikdagi matn bloklarini oddiy almashtirish algoritmi hisoblanadi.

**Basic block encryption algorithm** – the encoding algorithm that implements each fixed key value one reversible mapping from a set of plaintext blocks, having a fixed length. The algorithm is a simple replacement of blocks of text of fixed length.

**Алгоритм шифрования поточный** - алгоритм шифрования, реализующий при каждом фиксированном значении ключа последовательность обратимых отображений, действующую на последовательность блоков текста открытого.

**Oqimli shifrlash algoritmi** - kalitning har bir muayyan qiymatida ochiq matn bloklari ketma-ketligiga ta'sir etuvchi qaytariluvchi akslantirish ketma-ketligini amalga oshiruvchi shifrlash algoritmi.

**Stream encryption algorithm** - an encryption algorithm that implements, for each fixed value of key, sequence of reversible mapping that acting on a sequence of blocks of plaintext.

**Алгоритм шифрования** - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

**Shifrlash algoritmi** - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

**Encryption algorithm** - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

**Алгоритм кодирования имитозащищающего** - алгоритм криптографического преобразования информации, обеспечивающий контроль ее целостности (как правило за счет



внесения избыточности). В отличие от алгоритма формирования подписи цифровой использует криптосистемы симметричные. Примерами а. к. и. являются код аутентификации, некоторые автоматные преобразования и алгоритмы шифрования.

**Imitohimoyalovchi kodlash algoritmi** – axborot yaxlitligini (odatda, ortiqchalikni kiritish evaziga) nazoratlashni ta'minlovchi axborotni kriptografik o'zgartirish algoritmi. Raqamli imzoni shakllantirish algoritmidan farqli holda simmetrik kriptotizim ishlatiladi. Misol sifatida autentifikatsiyalash kodini, ba'zi avtomatik o'zgartirishlarni va shifrlash algoritmlarini ko'rsatish mumkin.

**Integrity protection coding algorithm** - the algorithm of cryptographic transformation of information, providing control its integrity (usually by introducing redundancy). In contrast to the algorithm for generating the digital signature uses a symmetric cryptosystem. Examples of the integrity protection coding algorithm are authentication code, some automatic conversion and encryption algorithms.

**Алгоритм криптографический** - алгоритм, реализующий вычисление одной из функций криптографических.

**Kriptografik algoritm** – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.

**Cryptographic algorithm** - the algorithm that implements the calculation of one cryptographic functions.

**Алгоритм расшифрования** - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.

**Deshifrlash algoritmi** – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

**Decryption algorithm** – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

**Алгоритм формирования подписи цифровой** - составная часть схемы подписи цифровой. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое

сообщение, ключ секретный, а также открытые параметры схемы подписи цифровой. Результатом работы алгоритма является подпись цифровая. В некоторых разновидностях схемы подписи цифровой при формировании подписи используется протокол.

**Raqamli imzoni shakllantirish algoritmi** – raqamli imzo sxemasining tarkibiy qismi. Kirish yo'liga imzolanuvchi xabar, maxfiy kalit, hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritm (umuman randomizatsiyalangan algoritm). Algoritm ishining natijasi raqamli imzo hisoblanadi. Raqamli imzo sxemasining ba'zi turlarida imzoni shakllantirishda protokol ishlatiladi.

**The algorithm for generating a digital signature** - an integral part of the digital signature scheme. The algorithm (generally randomized), the input of which serves a signed message, secret key and public parameters of the signature scheme digital. The result of the algorithm is the digital signature. In some versions of this signature scheme in the formation of the digital signature protocol is used.

**Алгоритм хеширования** - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

**Xeshlash algoritmi** – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

**Hashing algorithm** – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large



number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

**Алгоритм цифровой подписи** - асимметричный алгоритм, используемый для цифровой подписи данных.

**Raqamli imzo algoritmi** - ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

**Digital signature algorithm** – asymmetric algorithm used for digitally signing data.

**Алгоритм шифрования RSA** - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифросистем асимметричных.

**RSA shifrlash algoritmi** – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

**RSA encryption algorithm** - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

**Алгоритм шифрования инволютивный** - алгоритм шифрования, для которого алгоритмы шифрования и расшифрования совпадают. Другими словами, если к тексту открытому дважды применить алгоритм шифрования, то получится тот же самый открытый текст. Исторически для таких алгоритмов употребляется название «обратимый», но правильно называть их именно «инволютивными», в соответствии с общим пониманием инволюции в математике.

**Involyutiv shifrlash algoritmi** – shifrlash va deshifrlash algoritmlari bir xil bo'lgan shifrlash algoritmi. Boshqacha aytganda, agar ochiq matnga shifrlash algoritmi ikki marta qo'llanilsa, dastlabki ochik matn olinadi. Tarixan bunday algoritmlarga "qaytalanuvchi" iborasi ishlatiladi, ammo matematikadagi involyutsiya tushunchasiga mos holda aynan "involyutiv" iborasi ishlatilgani to'g'ri bo'ladi.

**Involutive encryption algorithm** - the encryption algorithm for which the encryption and decryption algorithms are the same. In other words, if the encoding algorithm is applied to the plaintext twice, we

get the same plaintext. Historically, such algorithms used the name "reversible", but the correct name for them is "involutive", in accordance with the common understanding of involution in mathematics.

**Алгоритм шифрования итеративный** - алгоритм шифрования, для которого соответствующие алгоритм шифрования и алгоритм расшифрования состоят из последовательных однотипных циклов шифрования.

**Iterativ shifrlash algoritmi** – mos shifrlash algoritmi va deshifrlash algoritmi shifrlashning ketma-ket bir xil sikllardan tashkil topgan shifrlash algoritmi.

**Iterative encryption algorithm** - the encryption algorithm for which the corresponding encoding algorithm and the decryption algorithm consist of sequential identical cycles of encryption.

**Атака на криптосистему** - попытка противника и/или нарушителя понизить уровень безопасности конкретной системы криптографической на основе определенных методов криптоанализа и при некоторых предположениях криптоанализа. Совокупность различных атак постоянно расширяется за счет развития теоретических методов и возможностей техники.

**Kriptotizimga hujum** – dushmanning va/yoki buzg'unchining kriptotahlilning ma'lum usullari asosida va kriptotahlilning ba'zi taxminlarida muayyan kriptografik tizim xavfsizligi darajasini pasaytirishga urinishi. Turli hujumlar majmui nazariy usullar va texnika imkoniyatlarining rivoji evaziga doimo kengaya boradi.

**The attack on the cryptosystem** - attempt of the opponent and/or the offender to decrease the level of security of specific cryptographic systems based on specific methods of cryptanalysis under certain assumptions cryptanalysis. The combination of different attacks is constantly expanding due to the development of theoretical methods and the potential of technology.

**Бит (двоичный код)** - минимальная единица количества информации в компьютере, равная одному двоичному разряду.



**Bit (ikkili kod)** – kompyuterdagi bitta ikkili xonaga teng axborot miqdorining minimal birligi.

**Bit (binary)** - the minimum unit of the amount of information in a computer, equal to one binary digit.

**Бит достоверности** - бит, добавляемый к слову в памяти компьютера для указания достоверности информации.

**Haqiqiylik biti** – axborot haqiqiyligini ko'rsatish maqsadida kompyuter xotirasidagi so'zga qo'shiladigan bit.

**Validity bit** - the bit added to the word in the computer memory to indicate the reliability of the information.

**Бит защиты** - двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи.

**Himoya biti** – xotiraning mos blokiga yozish yoki undan tanlash va unga yozishdan himoyalash uchun o'rnatiladigan xotira kalitidagi ikkili xona.

**Protection bit** - binary digit in the memory key setting protection of a corresponding memory block from write or from select and write.

**Бит контроля на четность** - контрольный бит, добавляемый к данным для контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данное, включая и единицу контрольного бита, всегда была четной (либо всегда нечетной).

**Juftlikka tekshirish biti** – ma'lumotlarga, ularning to'g'riligini nazorat qilish uchun ma'lumotni tashkil etuvchi ikkili birliklarning, jumladan, nazorat biti birligining yig'indigi doimo juft (yoki doimo toq) bo'lishligini ta'minlash maqsadida qo'shiladigan nazorat biti.

**Parity bit** - control bits added to the data to control their loyalty so that the sum of binary units, the components of this, including the unit control a bit, was always even (or always odd).

**Бит маски** - сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения или запрета определенных операций либо для проверки или изменения содержимого поля.

***Niqob biti*** – ma'lum amallar bajarilishiga ruxsat berish yoki rad etish yoki hoshiya tarkibini tekshirish yoki o'zgartirish uchun nol yoki bir qiymatiga o'rnatiluvchi bitlar birikmasi.

***Mask bit*** - the combination of bits set to zero or a single value to allow or prevent certain operations or to verify or modify the field contents.

***Блок*** – последовательность бинарных битов, которые включают ввод, вывод, состояние и раунд ключа. Длина последовательности - число битов, которые он содержит. Блоки также интерпретируются как массивы байтов.

***Blok*** – kalitning kirish, chiqish, holat va raundini o'z ichiga oluvchi binar bitlar ketma – ketligi. Ketma – ketlik uzunligi - u tashkil topgan bitlar soni. Bloklar baytlar massivlari shaklida ham izohlanadi.

***Block*** – sequence of binary bits that comprise the input, output, state, and round key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.

***Блок текста*** — мультиграмма текста (текста открытого, текста шифрованного или промежуточного), составленная из подряд идущих знаков. Обычно текст разбивается на блоки одинаковой длины.

***Matn bloki*** - ketma–ket keluvchi belgilardan tuzilgan matn multigrammasi (ochiq matn, shifrlangan matn, oraliq matn ). Odatda matn uzunligi bir xil bloklarga ajratiladi.

***Text block*** - multigram text (plaintext, ciphertext, or intermediate text), made up of consecutive digits. Usually the text is divided into blocks of equal length.

***Блокнот одноразовый*** — записанный на некотором материальном носителе (например, в специальных бумажных блокнотах) набор данных, используемых для получения последовательностей, управляющих для однократного шифрования. Этот набор данных, обладающий определенными свойствами, должен обеспечивать стойкость (шифрсистемы) совершенную при однократном применении.



***Bir martali bloknot*** - bir martali shifrlash uchun boshqaruvchi ketma-ketlikni olish maqsadida ishlatiluvchi qandaydir moddiy eltuvchida (masalan, maxsus qog'oz bloknotlarda) yozilgan ma'lumotlar nabori. Ma'lum xususiyatlarga ega bo'lgan ushbu ma'lumotlar nabori bir martali ishlatilishida mutlaqo bardoshlikni (kiriptotizim bardoshligini) ta'minlashi lozim.

***One-time pad*** - recorded on some tangible medium (e.g., special paper, notebooks) data set used to obtain the sequences of governors for a one-time encryption. This dataset, have certain properties that must ensure stability (cipher system) perfect after a single use.

***Блочный алгоритм шифрования*** - алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над *n*-битными блоками открытого текста.

***Shifrlashning blokli algoritmi*** – ochiq matnning *n*-bitli bloklari ustida kriptografik amallarni bajarish yo'li bilan dastlabki axborotning kriptografik o'zgartirishni amalga oshiruvchi shifrlash algoritmi.

***Block encryption algorithm*** - the encryption algorithm performing a cryptographic transformation of the original information by performing cryptographic operations on *n*-bit blocks of plain text.

***Гамма шифра*** - псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для шифрования открытой информации и расшифрования шифрованной.

***Shifr gammasi*** – ochiq axborotni shifrlash va deshifrlash uchun berilgan algoritm bo'yicha ishlab chiqiladigan psevdotasodifiy ikkili ketma-ketlik.

***Gamma cipher*** - pseudorandom binary sequence generated by a given algorithm for encoding public information and decrypt the encrypted.

***Гаммирование*** - процесс наложения по определенному закону гаммы шифра на открытые данные.

***Gammalash*** – ochiq ma'lumotlarga ma'lum qonuniyat bo'yicha gamma shifrini qo'yish jarayoni.

**Gamming** - the overlay process under the particular law of gamma cipher on the open data.

**Генератор ключей** - техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

**Kalitlar generatori** - kalit (kriptotizim kaliti), kalit ketma-ketligi, inisilizatsiya vektorlari va h.k. sifatida ishlatiluvchi son massivlari yoki boshqa ma'lumotlarni ishlab chiqarishga mo'ljallangan texnik qurilma yoki dastur.

**Key generator** - a technical device or program that is designed to generate arrays of numbers or other data used as a key (cryptosystem), the sequence of key, initialization vectors, etc.

**Генератор последовательностей псевдослучайных** — техническое устройство или программа для выработки последовательностей псевдослучайных.

**Psevdotasodifiy ketma-ketliklar generatori** - psevdotasodifiy ketma-ketliklarni ishlab chiqaruvchi texnik qurilma yoki dastur.

**Pseudorandom sequences generator** - a technical device or program to generate pseudorandom sequences.

**Дешифрование** - операция, обратная шифрованию и связанная с восстановлением исходного текста из шифрованного.

**Deshifrlash** – shifrlangan matnni dastlabki matnga tiklash bilan bog'liq shifrlashga teskari amal.

**Decryption** - the inverse operation of encryption and associated with the restoration of the original text from the encrypted.

**Ключ бинарный** — ключ, заданный вектором с двоичными координатами.

**Ikkili kalit** – ikkili koordinatali vektor ko'rinishida berilgan kalit.

**Binary key** — the key specified by the vector with integer coordinates.



**Ключ главный** — элемент ключа составного, который используется для шифрования ключей, предназначенных для шифрования ключей разовых или для генерации других видов ключей посредством шифрования определённых данных.

**Bosh kalit** - bir martali kalitlarni shifrlashga yoki ma'lum ma'lumotlarni shifrlash orqali kalitlarning boshqa turini generatsiyalash uchun mo'ljallangan kalitlarni shifrlashda ishlatiluvchi tarkibiy kalit elementi.

**Master key** — item composite key, used to encrypt keys for a single encryption key or to generate other types of keys through encryption of certain data.

**Ключ долговременный** — элемент ключей составных, действующий в неизменном виде длительное время.

**Davomli kalit** - uzoq vaqt davomida o'zgarmagan holda ishlatiluvchi tarkibiy kalit elementi.

**Long-term key** — item composite key, valid unchanged for a long time.

**Ключ шифрования** — ключ, используемый при шифровании.

**Shifrlash kaliti** - shifrlashda ishlatiluvchi kalit.

**Encryption key** — the key used in the encoding.

**Ключ шифрованный** - криптографический ключ, который был шифрован с помощью аттестованной функции безопасности с ключом ключа шифрования, ПИН-кода или пароля для того, чтобы скрыть значение базового ключа открытого текста.

**Shifrlangan kalit** - ochiq matnning bazaviy kaliti qiymatini yashirish maqsadida attestatsiyadan o'tgan xavfsizlik funksiyasi bilan kalitni shifrlash kaliti, PIN kod yoki parol yordamida shifrlangan kriptografik kalit.

**Encrypted key** – a cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

**Ключ симметричный** - криптографический ключ, использующийся для выполнения как криптографической операции и её инверсии, например, для шифрования и дешифрования, или создать код аутентификации сообщения и проверки кода.

**Simmetrik kalit** - har ikkala, kriptografik amal va uning inversiyasini, masalan, shifrlash va deshifrlashni yoki xabarni autentifikatsiyalash kodini hosil qilish va kodni tekshirishni amalga oshirish uchun foydalaniluvchi kriptografik kalit.

**Symmetric key** – a cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

**Ключ слабый** — ключ криптосистемы, при котором заметно ухудшаются характеристики стойкости криптографической криптосистемы по сравнению со средними значениями тех же характеристик при ключе, случайно равновероятно выбранном из множества ключевого криптосистемы.

**Zaif kalit** - kriptotizim kaliti bo'lib, unda kriptotizimning kriptobardoshlik xarakteristikalari, kriptotizim kalitlari to'plamidan tasodifan, teng ehtimollik tarzda tanlangan kalitning o'sha xarakteristikalarining o'rtacha qiymatlariga nisbatan sezilarli darajada yomonlashadi.

**Weak key** — key cryptosystem, which significantly degraded the strength of cryptographic cryptosystem in comparison with the average values of the same characteristics when key randomly uniformly chosen from the set key of the cryptosystem.

**Код аутентификации** — вид алгоритма кодирования имитозащищающего информации. Как правило, код аутентификации сопоставляет сообщение с его кодом аутентичности. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения.

**Autentifikatsiya kodi** – axborotni imitohimoyalovchi kodlash algoritmining turi. Odatda, autentifikatsiya kodi xabarni uning haqiqiylik kodi bilan taqqoslaydi. Axborotning haqiqiyligi xususida



qaror qabul qilish algoritmi xabar haqiqiyligi kodi qiymatini tekshirishga asoslangan.

**Authentication code** — the type of encoding algorithm mitsamiouli information. Typically, the authentication code matches the message code authenticity of the message. The decision algorithm on the authentication information based on the verification code value to the authenticity of the message.

**Код аутентификации сообщений на основе хэш** - код аутентификации сообщения, использующий криптографический ключ в сочетании с хэш-функцией.

**Xeshga asoslangan xabarlarni autentifikatsiyalash kodi** - xesh funksiya bilan birgalikda kriptografik kalitdan foydalanuvchi, xabarlarni autentifikatsiyalash kodi.

**Hash-based message authentication code** – a message authentication code that uses a cryptographic key in conjunction with a hash function.

**Коды Рида Соломона** - важное семейство линейных блоковых кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут рассматриваться и как обобщение кодов Боуза Чоудхури Хокенгема, и как особый случай кодов Гоппы, могут быть отнесены к циклическим кодам.

**Rid Solomon kodlari** – xatoliklarni tuzatuvchi, ayniqsa, xatoliklar paketini tuzatishga qulay chiziqli blokli kodlarning muhim oilasi. Ushbu kodlarni Bouz Choudxuri Xokengem kodlarining umumlashtirilgani sifatida va Goppa kodlarining maxsus holi sifatida, siklik kodlar sifatida ko'rish mumkin.

**Reed - Solomon codes** - an important family of linear block codes with error correction particularly useful for correcting error bursts. They can be considered as a generalization of codes Bose Chowdhury of Hockenheim, and as a special case codes happy, can be related to cyclic codes.

**Коллизия** – два или больше разных типов ввода, которые осуществляют одинаковый вывод.

**Kolliziya** – ikki yoki undan ortiq turli kirishlarni bir xil chiqish hosil qilishi.

**Collision** – two or more distinct inputs produce the same output.

MUNDARIJA

XUDOYKULOV Z.T., ISLOMOV SH.Z., MARDIYEV U.R.

# KRIPTOGRAFIYA 1

## O‘quv qo‘llanma

Toshkent - “METODIST NASHRIYOTI” - 2024

*Muharrir: Bakirov Nurmuhammad*

*Texnik muharrir: Tashatov Farrux*
*Musahhih: Shoumarova Oqila*
*Dizayner: Ochilova Zarnigor*

*Bosishga 1.04.2024.da ruxsat etildi.*
*Bichimi 60x90. “Times New Roman” garniturasi.*
*Ofset bosma usulida bosildi.*
*Shartli bosma tabog‘i 14 Nashr bosma tabog‘i 13,5.*
*Adadi 300 nusxa.*

*“METODIST NASHRIYOTI” MCHJ matbaa bo‘limida chop etildi.*
*Manzil: Toshkent shahri, Shota Rustaveli 2-vagon tor ko‘chasi, 1-uy.*

*+99893 552-11-21*



ISBN 978-9910-03-246-2