

MIRZO ULUG'BEK NOMIDAGI
O'ZBEKISTON MILLIY UNIVERSITETI



G.U.JO'RAYEV

KRIPTOGRAFIK PROTOKOLLAR

03b.2
68
1-98

**O‘ZBEKISTON RESPUBLIKASI
OLIY VA O‘RTA MAXSUS TA‘LIM VAZIRLIGI**

**MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI**

G.U.JO‘RAYEV

KRIPTOGRAFIK PROTOKOLLAR

O‘quv qo‘llanma

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta‘lim vazirligi
70610301 – “Kriptografiya va kriptanaliz” hamda
70610302 – “Axborot xavfsizligi” magistratura mutaxassisliklari
uchun o‘quv qo‘llanma sifatida tavsiya etgan

**O‘ZMU
MATEMATIKA
FAKULTETI
ARM**

**Toshkent
“Universitet”
2022**

UO*K: 004.56:003.26(075.8)

KBK: 32.811.4ya73

J 96

G.U.Jo'rayev. Kriptografik protokollar. O'quv qo'llanma.

-T.: "Universitet", 2022. 160 bet.

Mazkur o'quv qo'llanmada elektron raqamli imzo, autentifikasiyalash va identifikasiyalash, oshkoraligi nol bo'lgan, sirni taqsimlash, shifrlash kalitlarini generatsiya qilish va boshqarish, tanga tashlash protokollari hamda kriptografik protokollarga qilinadigan asosiy hujum turlari va ularni bartaraf qilish, elektron to'lovlar va yashirin ovoz berish xavfsizligini ta'minlashda kriptografik protokollarni qo'llash masalalari bayon qilingan.

Ushbu o'quv qo'llanma 60610300 – Axborot xavfsizligi ta'lim yo'nalishi talabalariga mo'ljallangan. O'quv qo'llanma axborot texnologiyalari sohasi talabalari va mutaxassislari uchun ham foydali bo'lishi mumkin.

UO*K: 004.56:003.26(075.8)

KBK: 32.811.4ya73

J 96

Taqrizchilar:

M.M.Karimov – texnika fanlari doktori, professor

R.D.Aloyev – fizika-matematika fanlari doktori, professor

O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligining 2022 yil 13 maydagi 166-sonli buyrug'iga asosan nashr qilish uchun tavsiya etilgan.

ISBN: 978-9943-8695-3-0

© "Universitet" nashriyoti, Toshkent

MUNDARIJA

KIRISH	8
1-BOB. KRIPTOGRAFIK PROTOKOLLAR HAQIDA DASTLABKI MA'LUMOTLAR	12
§1.1. Asosiy tushunchalar.....	12
§1.2. Kriptografik protokollar klassifikatsiyasi.....	14
§1.3. Kriptografik protokollarni zaifligi.....	16
§1.4. Kriptografik protokol zaifligiga oid misollar.....	17
§1.5. Kriptografik protokollarga nisbatan keng tarqalgan hujum turlari ...	20
2-BOB. KRIPTOGRAFIK PROTOKOLLAR VA ULARNING XAVFSIZLIGIGA QILINADIGAN ASOSIY HUJUMLAR	22
§2.1. Shamir–Rivest–Adleman protokoli.....	22
§2.2. Diffi–Xellman protokoli.....	23
§2.3. Masumoto–Takashima–Imai (MTI) protokoli.....	24
§2.4. STS protokoli.....	26
3-BOB. AUTENTIFIKASIYALASH VA IDENTIFIKASIYALASH PROTOKOLLARI	29
§3.1. Autentifikatsiyalash va identifikatsiyalashning asosiy tushunchalari.....	30
§3.2. Autentifikatsiyalash usullari.....	34
§3.3. Autentifikatsiyalash protokollari turlari.....	37
§3.4. Parol bo'yicha autentifikatsiyalashga hujumlar va ularni bartaraf qilish.....	40
§3.5. Foydalanuvchini autentifikatsiya qilishning Lamport protokoli.....	44
§3.6. «Savol-javob» turidagi autentifikatsiyalash protokollari.....	45
§3.7. Simmetrik kriptosxemalardan foydalanuvchi «savol-javob» protokollari.....	46
§3.8. Kerberos protokoli.....	48
§3.9. Elektron raqamli imzodan foydalanuvchi protokollar.....	54
§3.10. Ochiq shifrlash sxemalariga asoslangan o'zaro autentifikatsiyalash protokoli.....	55
§3.11. «Savol-javob» turidagi o'zaro identifikatsiyalash protokollari.....	56
§3.12. 1– «qo'l siqishish» protokoli.....	57
§3.13. 2– «qo'l siqishish» protokoli.....	59
4-BOB. ISBOTI NOL OSHKORALIKKA ASOSLANGAN AUTENTIFIKASIYALASH PROTOKOLLARI	60
§4.1. Oshkoraligi nol bo'lgan protokollar.....	60
§4.2. Ali Bobo g'ori nolli oshkoralikka misol sifatida.....	63
§4.3. Fiat –Shamirning autentifikatsiyalash protokoli.....	66
§4.4. Autentifikatsiyalashning Schnorr sxemasi.....	69
§4.5. Autentifikatsiyalashning Brikell va MakKarli sxemasi.....	70

§7.15. Diffi-Xellman protokoli.....	112
§7.16. Nidkem-Srederning transport protokoli	114
§7.17. X-509 standarti	114
8-BOB. ELEKTRON RAQAMLI IMZO PROTOKOLLARI	116
§8.1. Elektron raqamli imzo	116
§8.2. Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli.....	118
§8.3. Ochiq kalitli kriptografiyadan foydalanib, hujjatlarni imzolash.....	120
§8.4. Maxsus algoritmlar, ya'ni ERI protokollari asosida hujjatlarni imzolash.....	123
9-BOB. ELEKTRON TO'LOVLAR XAVFSIZLIGINI TA'MINLASHDA KRIPTOGRAFIK PROTOKOLLARNI QO'LLASH	130
§9.1. Elektron to'lovlar tizimining umumiy sxemasi.....	130
§9.2. RSA raqamli imzodan foydalanib, elektron to'lovlar xavfsizligini ta'minlash	132
§9.3. Elektron to'lovlar xavfsizligining «ko'r-ko'rona» imzoga asoslangan sxemasi	133
§9.4. Elektron to'lovlar xavfsizligining bir tomonlama funksiyaga asoslangan sxemasi.....	136
§9.5. Turli xil qiymatga ega bo'lgan banknotlar uchun elektron to'lov sxemasi	137
§9.6. Bir xil qiymatga ega bo'lgan elektron banknotlar uchun Shaum sxemasi	138
10-BOB. YASHIRIN OVOZ BERISH PROTOKOLI VA UNING KRIPTOGRAFIK TAVSIFI	142
§10.1. Yashirin ovoz berish jarayoni.....	142
§10.2. Aloqaning telekommunikasiya kanallari bo'yicha ochiq kalitli kriptografiyaga asoslangan yashirin ovoz berish protokoli	145
§10.4. Yashirin ovoz berish protokoliga qo'shimcha sharhlar	155
FOYDALANILGAN ADABIYOTLAR RO'YXATI.....	157

§4.6. Gillu-Kiskate protokoli.....	71
§4.7. Okamoto protokoli.....	72
§4.8. Feyge-Fiat-Shamir protokoli	73
§4.9. RSA kriptotizimiga asoslangan protokol	75
§4.10. Bir raundli tekshirishga asoslangan protokol.....	76
5-BOB. TANGA TASHLASH PROTOKOLLARI.....	78
§5.1. Tanga tashlash sxemalari.....	78
§5.2. Blyum – Mikal protokoli.....	79
§5.3. Diskret logarifmlashga asoslangan tanga tashlash protokoli	80
§5.4. RSA kriptotizimi asosidagi tanga tashlash protokoli.....	80
§5.5. Shnorr kriptotizimi asosidagi tanga tashlash protokoli.....	81
§5.6. Tasodifiy umumiy bitni hosil qilish uchun diskret logarifmlashga asoslangan tanga tashlash protokoli	82
6-BOB. SIRNI TAQSIMLASH PROTOKOLLARI.....	83
§6.1. Sirlarni taqsimlashning asosiy tushunchalari	83
§6.2. Sirni taqsimlashning bo'sag'ali sxemalari	84
§6.3. Lagranj interpolyasion ko'phadiga asoslangan Shamir sxemasi	87
§6.4. Qoldiq haqidagi Xitoy teoremasiga asoslangan sirni taqsimlash sxemasi	89
§6.5. Ixtiyoriy tuzilmaga ega bo'lgan guruhlar o'rtasida sirni taqsimlash	91
§6.6. Taqsimlangan sirni tekshirish sxemasi.....	92
7-BOB. SHIFRLASH KALITLARINI GENERASIYA QILISH VA BOSHQARISH	96
§7.1. Shifrlash kalitlari uzunligi.....	96
§7.2. Seansli kalitlarni generasiya qilish.....	98
§7.3. Simmetrik shifrlash algoritmlari uchun kalitli axboratlarni generasiya qilish	99
§7.4. Asimmetrik (ochiq kalitli) shifrlash algoritmlari uchun kalitli axboratlarni generasiya qilish.....	101
§7.5. Kalitlarni saqlash.....	101
§7.6. Kalitlarni tarqatish sxemalari	102
§7.7. Kalitlarni markazlashgan tarqatish.....	104
§7.8. Simmetrik kriptografiyadan foydalanib, ishonchli markaz tomonidan maxfiy kalitlarni tarqatish protokoli.....	106
§7.9. Wide-Mouth Frog protokoli.....	106
§7.10. Yahalom protokoli.....	107
§7.11. Nidkem-Shreder protokoli.....	108
§7.12. Orvey-Riis protokoli.....	109
§7.13. Ikki kalitli kriptografiyadan foydalanib, kalitlarni tarqatish	110
§7.14. Shamirning kalitsiz protokoli	111

Kriptografik protokollarning umumiy qoidasi: protokolda belgilanganidan ortiqcha harakatlarni qilish yoki axborotlarni bilish mumkin emas.

Hozirgi vaqtda axborot xavfsizligining turli masalalarini ijobiy hal qilishda kriptografik protokollar muvaffaqiyatli qo'llanilmoqda. Bunda ushbu sohadagi o'quv adabiyotlarining o'rni beqiyos katta. Shu bois, kompyuter texnologiyalari sohasining tegishli yo'nalishlarida ta'lim olayotgan talabalar, ayniqsa, 60610300 – – Axborot xavfsizligi ta'lim yo'nalishi va unga mos magistratura mutaxassisliklari talabalari bu fanni chuqur o'zlashtirishlari va uni amaliyotga qo'llay olishlari katta ahamiyat kasb etadi.

Ushbu «Kriptografik protokollar» o'quv qo'llanmasi muallifning mazkur nomdagi 2016 yilda bosmadan chiqarilgan o'quv qo'llanmasiga ayrim tuzatish va qo'shimchalar kiritish orqali yaratildi. Shuningdek, uni tayyorlashda kriptografik protokollarga doir rus tilida nashr qilingan o'quv adabiyotlari va chet el manbalaridan keng foydalanildi.

G.U. Jo'rayev

SO'Z BOSHI

Shifrlash kalitlarini ochiq taqsimlash masalasi hamda elektron raqamli imzolarni amaliyotga qo'llanilishini muvaffaqiyatli hal qilinishi kriptografiyada kriptografik protokollar nazariyasi deb nomlanuvchi yangi yo'nalishni paydo bo'lishiga katta turtki bo'ldi. Buning natijasida qandaydir amaliy masalani yechish maqsadida bir-birlari bilan ochiq aloqa kanali orqali axborot almashinuvchi foydalanuvchilar kriptografik protokollar nazariyasining ob'yekti sifatida xizmat qiladi.

Dastlabki kriptografik protokollar XX asrning ikkinchi yarmida, aniqrog'i 1970-yillarning oxirida paydo bo'lgan. Hozirgi kunda turli xildagi bir necha o'nlab kriptografik protokollar mavjud. Ularni quyida keltirilgan 2 ta toifaga ajratish mumkin:

1. *Amaliy protokollar.* Bu toifadagi protokollar amaliyotda uchraydigan konkret masalalardan birini yechishga mo'ljallangan bo'ladi.
2. *Primitiv protokollar.* Ushbu protokollar amaliy protokollarni amalga oshirishda amaliy protokollarning qurilish bloki sifatida xizmat qiluvchi protokollardir. Ya'ni, primitiv protokollar mustaqil amaliy ahamiyatga ega bo'lmaydi. Shifrlash algoritmlari, xesh funksiyalar, tanga tashlash va sirlarni taqsimlash sxemalari primitiv protokollarga misol bo'ladi.

Amaliy kriptografik protokollar quyidagi masalalarni hal qilishda muvaffaqiyatli qo'llanilmoqda:

- elektron to'lovlar;
- ma'lumotlarni elektron almashish;
- elektron tijorat;
- elektron ovoz berish.

Protokollarda kriptografik elementlar yoki algoritmlarni qo'llanilishidan maqsad buzg'unchilik va firibgarlikni oldini olish yoki aniqlashdan iborat. Kriptografik protokollarda shifrlash algoritmlari ishlatilsa-da, lekin uning maqsadi konfidentsiallik yoki maxfiylikni ta'minlash bo'lishi shart emas. Masalan, ko'p hollarda protokolda ishtirok etuvchi tomonlar bir vaqtning o'zida qandaydir kontraktni imzolash, elektron qur'a tashlash, poker kabi o'yinlarda ishtirok etishlari ham mumkin.

Bugungi kunda ko'plab odamlar «yuzma-yuz» muomala qilmasdan, kompyuter tarmog'i orqali muomala qilishmoqda. Insonlar muomalasidagi ko'plab protokollarning xavfsizligi va halol (g'irromsiz) ligi ularni muomalada shaxsan yoki «yuzma-yuz» ishtirok etishlariga asoslangan. Masalan, o'zi ishonmagan odamga bozordan xarid qilib kelish uchun hech kim pul bermaydi. Shuningdek, saylovda o'ziga ma'qul bo'lgan nomzodga ovoz berish uchun ovoz berish byulletenini begonaga bermaslik ushbu jarayonlarda harakatlarni amalga oshirishda g'irromlikga yo'l qo'ymaslik maqsadida yoki xavfsizlik nuqtai nazaridan ishtirokchining shaxsan o'zi protokolni amalga oshirishi lozim bo'ladi.

Kompyuter tarmog'idan foydalanuvchilar va ushbu tarmoqni ishlab chiquvchilarning hammasini ham halol deb bo'lmaydi. Ularni ko'pchiligi qandaydir zararlarni keltirib chiqarishga urinadilar. Shu sababli kompyuter tarmoqlarida bunday zararlarni oldini olish maqsadida kriptografik protokollar keng qo'llanilmoqda [9,10].

Kriptografik protokol (inglizcha cryptographic protocol) - bu kriptografik algoritmlar naborini o'z ichiga oluvchi abstrakt yoki konkret protokoldir. Kriptografik almashtirish va algoritmlardan foydalanish qoidalari nabori protokollar asosini tashkil qiladi [10].

Kriptografik usullar vositasida axborot xavfsizligini ta'minlash tizimi *kriptografik tizim deyiladi*.

Har xil kriptografik protokollarni qo'llash natijasida kriptografik tizim xavfsizlikning turli funksiyalarini bajarishi mumkin. Kriptografik protokollarning asosiy funksiyalari esa quyidagilardan iborat bo'lishi mumkin [1-3,7-9,11]:

Ma'lumotlar konfidensialligi yoki maxfiyligini ta'minlash.

Ma'lumotlar manbaini autentifikasiyalash.

Axborot almashinuvida ishtirok etuvchilarni autentifikasiyalash.

Qabul qilishni isbotlash yo'li bilan rad etishga yo'l qo'ymaslik.

Manbaini isbotlash yo'li bilan rad etishga yo'l qo'ymaslik.

Ma'lumotlar butunligini ta'minlash.

Primitiv kriptografik protokollar mustaqil ravishda amaliy ahamiyatga ega bo'lmaydi. Shu bois ushbu turdagi protokollar amaliy kriptografik protokollarni komponenti sifatida xizmat qiladi. Primitiv kriptografik protokollar qandaydir abstrakt masalani yechishga

KIRISH

Ikki yoki undan ortiq tomonlar tomonidan aniq bir masalani yechish uchun qabul qilinadigan harakatlar tartibi *protokollar deyiladi* [3-6]. «Harakatlar tartibi» iborasi shuni anglatadiki, protokollar boshidan oxirigacha ma'lum bir ketma-ketlikda amalga oshiriladi. Har bir harakat faqatgina oldingisi amalga oshirilgandan keyingina o'z navbatida bajariladi.

«Ikki yoki undan ortiq tomonlar tomonidan qabul qilinadigan» iborasi shuni anglatadiki, protokollarni amalga oshirishda kamida ikkita odam ishtirok etadi. Bitta odam protokolni amalga oshirolmaydi. U masalani yechishda ma'lum bir harakatlarni bajarishi mumkin. Masalan, biror kishi tort sotib olsa (bu holda u ma'lum bir masalani hal qildi deb hisoblash mumkin), ammo bu protokol emas. Haqiqiy protokol bo'lishi uchun kimdir tortni eyishi (tortni ta'mi haqida aniq fikr bildirishi) lozim bo'ladi [3].

Har qanday protokol qandaydir natijaga olib kelishi kerak. Shu sababli ta'rifda «aniq bir masalani yechish uchun» iborasi ishlatiladi.

Protokollar quyida keltirilgan boshqa xususiyatlarga ham ega:

- protokolda ishtirok etuvchilarning har biri protokolni va uni tashkil etuvchi harakatlar ketma-ketligini bilishi lozim;
- protokolda ishtirok etuvchilarning har biri protokolga amal qilishga rozi bo'lishlari lozim;
- protokol ziddiyatli bo'lmasligi lozim, ya'ni protokoldagi har bir harakat shunday aniqlanishi kerakki, uni amalga oshirish jarayonida tushunmovchiliklar kelib chiqmasligi lozim;
- protokol to'liq bo'lishi lozim, ya'ni protokolda bo'lishi mumkin bo'lgan har bir vaziyat yoki holat ma'lum bir harakatga mos bo'lishi lozim.

Kundalik hayotda norasmiy protokollar ko'plab uchrab turadi: telefon orqali tovarlar va chiptalarga buyurtma berish, saylovlarda ishtirok etish, turli xil o'yinlarda ishtirok etish. Bu harakatlar amalda protokollar ekanligi haqida hech kim o'ylab ham ko'rmagan, ammo ular uzoq vaqtlar davomida ishlab chiqilgan va ulardan foydalanishni hamma yaxshi biladi.

6-bobda oshkoraligi nol bo'lgan protokollar bayon qilingan. Xususan, Fiat-Shamir, Feige-Fiat-Shamir, RSA kriptotizimiga va bir raundli tekshirishga asoslangan protokollar o'rganilgan.

Sirlarni taqsimlashning asosiy tushunchalari, sirni taqsimlashning bo'sag'ali sxemalari, Lagranj interpolyasion ko'phadiga asoslangan Shamir, qoldiq haqidagi Xitoy teoremasiga asoslangan sxemalari hamda ixtiyoriy tuzilmaga ega bo'lgan guruhlar o'rtasida sirlarni taqsimlash va taqsimlangan sirni tekshirish masalalari o'quv qo'llanmasining 7-bobida bayon qilingan.

8-bobda shifrlash kalitlarini generasiya qilish va boshqarish masalalari o'rganilgan. Xususan, unda seansli kalitlarni generasiya qilish, simmetrik va ocik kalitli shifrlash algoritmlari uchun kalitli axborotlarni generasiya qilish, kalitlarni saqlash va tarqatish masalalariga keng o'rin berilgan hamda ularga oid bir necha protokollar keltirilgan.

O'quv qo'llanmasining 9-bobi elektron to'lovlar xavfsizligini ta'minlashda kriptografik protokollarni qo'llash masalasiga bag'ishlangan. Ushbu bobda elektron to'lovlar tizimining umumiy sxemasi keltirilgan. Shuningdek, RSA, «ko'r-ko'rona» raqamli imzolar va bir tomonlama funksiyaga asoslangan elektron to'lovlar xavfsizligini ta'minlash sxemalari bayon etilgan. Bir va turli xil qiymatlarga ega bo'lgan elektron banknotlar uchun elektron to'lov sxemalari o'rganilgan.

Hozirgi kundalik hayotda insonlar o'rtasida turli xil bahs va munozaralarga asoslangan muammolar tanga tashlash yoki qur'a o'tkazih yo'li bilan oson hal qilinmoqda. Shu bois, tanga tashlash yo'li bilan elektron qur'a o'tkazih kriptografiyada ham muhim o'rin egallaydi. Qo'llanmaning 10-bobida tanga tashlashning bir necha protokollari hamda tasodifiy umumiy bitni hosil qilish uchun diskret logarifmlashga asoslangan tanga tashlash protokoli keltiriladi.

yo'naltirilgan bo'ladi. Sirlarni taqsimlash, bitga bog'lab qo'yish, tanga tashlash protokollari primitiv kriptografik protokollarga misol bo'ladi.

Amaliy kriptografik protokollar kriptotizimlar yordamida axborot xavfsizligini ta'minlashning konkret amaliyot masalalarini yechish uchun mo'ljallangan. Bu turdagi protokollarga misol sifatida elektron to'lov, ma'lumotlarni elektron almashinuv tizimlari hamda elektron hujjat aylanish, ovoz berish (elektron saylov), qur'a tashlash, poker o'yini kabi protokollarni misol keltirish mumkin.

O'quv qo'llanmasining 1-bobida kriptografik protokollarga oid tushunchalar, xususan, kriptografik protokollarni klassifikatsiyalash, kriptografik protokollarni zaifligi va kriptografik protokollarga nisbatan keng tarqalgan hujum turlari bayon qilinadi.

2-bobda Shamir-Rivest-Adleman, Diffi-Xellman, Masumoto-Takashima-Imai (MTI) va STS protokollari misolida kriptografik protokollar va ularning xavfsizligiga qilinadigan asosiy hujumlar keltiriladi.

Elektron raqamli imzo tushunchasi, simmetrik kriptotizim va uchinchi shaxs ishtirokidan hamda ochiq kalitli kriptotizimlardan foydalanib, hujjatlarni imzolash protokollari, shuningdek, elektron raqamli imzo standartlarida qo'llaniladigan maxsus algoritmlar – DSA va GOST R 34.10-2001 elektron raqamli imzo algoritmlari 3-bobda muhokama qilingan.

O'quv qo'llanmasining 4-bobida hozirgi kunda amaliyotga keng qo'llanilayotgan autentifikatsiyalash va identifikatsiyalash protokollari keltirilgan. Xususan, ushbu bobda foydalanuvchini autentifikatsiya qilishning Lamport va Kerberos protokollari, «savol-javob» turidagi autentifikatsiyalash, elektron raqamli imzodan foydalanuvchi, ochiq shifrlash sxemalariga asoslangan o'zaro autentifikatsiyalash, «qo'l siqishish» protokollari bayon qilinadi.

Isboti nol oshkoralikka asoslangan autentifikatsiyalash protokollariga misol sifatida o'quv qo'llanmasining 5-bobida Fiat-Shamir, Gillu-Kiskate, Okamoto protokollari hamda Shnor, Brikell va MakKarli sxemalari keltirilgan.

- xabarni qabul qilish va jo'natish.

Protokol qadamlari ketma-ketligi protokol siklini tashkil qiladi. Ikki ishtirokchi asosidagi kriptografik protokollarda sikl deyilganda faqatgina bitta ishtirokchi faol bo'lgan vaqt oralig'ida bajarilgan qadamlar (harakatlar) ketma-ketligi tushuniladi. Sikl bir (faol) ishtirokchi tomonidan xabarni shakllantirish va jo'natish orqali faollikni boshqa ishtirokchiga o'tishi bilan tugallanadi.

Konkret ishtirokchilarning aniq bir protokolni amalga oshirishi *seans deb nomlanadi*.

Seans doirasida protokolning har bir ishtirokchisi bir yoki bir necha rollarni bajarishi mumkin. Protokolning boshqa seansida ishtirokchilar rollarni almashishlari va boshqa funksiyalarni bajarishlari mumkin.

Misol. Maxfiy axborot almashinuv protokoli.

Sikl №1:

1-chi qadam: A ishtirokchi M_1 xabarni shakllantiradi.

2-chi qadam: A ishtirokchi $S_1 = E_{k_{AB}}(M_1)$ ni hisoblaydi.

3-chi qadam: A ishtirokchi B ishtirokchiga S_1 xabarni jo'natadi.

4-chi qadam: B ishtirokchi S_1 xabarni qabul qiladi va xabardan A jo'natuvchining identifikatorini biladi.

5-chi qadam: B ishtirokchi $M_1 = D_{k_{AB}}(S_1)$ matnini hosil qiladi.

Sikl №2:

1-chi qadam: B ishtirokchi M_2 xabarni shakllantiradi.

2-chi qadam: B ishtirokchi $S_2 = E_{k_{BA}}(M_2)$ ni hisoblaydi.

3-chi qadam: B ishtirokchi A ishtirokchiga S_2 xabarni jo'natadi.

4-chi qadam: A ishtirokchi S_2 xabarni qabul qiladi va xabardan B jo'natuvchining identifikatorini biladi.

5-chi qadam: A ishtirokchi $M_2 = D_{k_{BA}}(S_2)$ matnini hosil qiladi.

Ushbu protokolni quyidagi sxematik ko'rinishda osongina ifodalash mumkin:

$$(1) A \rightarrow B: E_{k_{AB}}(M_1),$$

$$(2) A \leftarrow B: E_{k_{BA}}(M_2).$$

Ko'pgina mavzularni bayon qilishda protokolni aynan mana shu sxematik ko'rinishidan foydalaniladi.

1-BOB. KRIPTOGRAFIK PROTOKOLLAR HAQIDA DASTLABKI MA'LUMOTLAR

Ushbu bobda kriptografik protokollarga oid tushunchalar, xususan, kriptografik protokollarni klassifikatsiyalash, kriptografik protokollarni zaifligi va kriptografik protokollarga nisbatan keng tarqalgan hujum turlari bayon qilinadi.

§1.1. Asosiy tushunchalar

Protokolni ishtirokchilari (ayrim o'rinlarda sub'ekt yoki tomonlar ham deb nomlanadi) sifatida nafaqat foydalanuvchi yoki abonentlar, balki mijoz va server ilovalari rolini bajaruvchi jarayonlar ham qatnashishlari mumkin.

Kriptografik protokolda ishtirok etuvchilarning har biri protokolni amalga oshirish jarayonida quyidagi harakatlarni bajarishlari mumkin:

➤ protokolni boshqa ishtirokchisiga yoki ishtirokchilariga xabarlar jo'natishi;

➤ boshqa ishtirokchidan xabarlar qabul qilishi;

➤ quyida keltirilgan ichki harakatlarni

- qandaydir hisoblashlarni bajarishi;

- qandaydir shartlarni tekshirishi;

- o'zgaruvchilarni qiymatlarini yangilashi.

Kriptografik protokollarda sikl, qadam va seans tushunchalaridan keng foydalaniladi.

Protokolning sikli (inglizcha *round*) protokoldagi faqat bitta ishtirokchi faol bo'ladigan vaqt oralig'ini anglatadi. Sikl o'z navbatida qadam (inglizcha *step, action*) lardan tashkil topadi. Protokolning konkret ishtirokchisi tomonidan sikl jarayonida tugallangan harakat *protokol qadami deb nomlanadi*. Masalan, kriptografik protokol qadami sifatida quyida keltirilgan harakatlardan biri bo'lishi mumkin:

- tasodifiy sonni generatsiya qilish;

- xabarni jo'natish;

- qandaydir funksiyani qiymatini hisoblash;

- xabar yoki kalitni shifrlash;

- sertifikat, kalit, imzo va boshqalarni tekshirish;

autentlik xossalarini ta'minlash uchungina ishlatilsa, arxivlash amali bajarilmasligi ham mumkin. Bu holda tekshiruvdan so'ng yoki ma'lum bir chegaralangan vaqtdan keyin ERI yo'q qilinishi mumkin.

Identifikasiyalash (autentifikasiyalash) protokollari.

Identifikasiyalash protokoli asosida qandaydir nom (identifikator) ni taqdim etgan identifikasiyalanuvchi ob'ekt (masalan, ob'ekt, qurilma, jarayon...) qandaydir maxfiy ma'lumotni bilishini tekshirishuvchi algoritmdan foydalanishga asoslangan. Tekshirish jarayoni maxfiy ma'lumot oshkor qilinmasdan amalga oshiriladi.

Ayrim hollarda identifikasiyalash protokoli autentifikasiyalash protokoligacha kengaytirilishi mumkin. Bunda identifikasiyalanuvchi ob'ekt buyurtirilayotgan xizmatlarga vakolati bor yoki yo'qligi tekshiriladi.

Agar identifikasiyalash protokolida ERI ishlatilsa, u holda maxfiy ma'lumot sifatida ERIni maxfiy kaliti ishlatiladi, ERIni tekshirish ERIning ochiq kaliti yordamida amalga oshiriladi.

Autentifikasiyalangan kalitlarni taqsimlash protokollari. Bu turdagi protokollar 3 ta ishtirokchi tomonidan amalga oshiriladi. Uchinchi ishtirokchi sifatida kalitlarni generasiya qiluvchi va tarqatuvchi, server deb nomlanuvchi S markaz ishtirok etadi. Ushbu turdagi protokollar generasiya qilish, qayd qilish va kommunikasiya deb nomlanuvchi 3 bosqichda amalga oshiriladi. Birinchi bosqichda server S tizimning sonli parametrlari, shu jumladan, o'zining ochiq va yopiq kalitini generasiya qiladi.

Qayd qilish bosqichida server S hujjatlar bo'yicha foydalanuvchilarni (ular yoki ularni vakolatli shaxslari ishtirokida) identifikasiyalaydi. Har bir ob'ekt uchun kalitli yoki identifikasiyalash ma'lumotlarini generasiya qiladi hamda tizimning sonli qiymatlaridan (zarurat bo'lganda server S ning ochiq kalitidan ham) iborat bo'lgan xavfsizlik belgilarini shakllantiradi.

Kommunikasiya bosqichida umumiy seans kalitini shakllantirish bilan tugaydigan autentifikasiyalangan kalit almashish protokoli amalga oshiriladi.

§1.2. Kriptografik protokollar klassifikasiyasi

Foydalanish turiga ko'ra kriptografik protokollar quyidagicha klassifikasiyalanadi [3,5-7,11]:

Shifrlash (dastlabki matnga o'girish) protokollari.

Elektron raqamli imzo (ERI) protokollari.

Identifikasiyalash/autentifikasiyalash protokollari.

Autentifikasiyalangan kalitlarni taqsimlash protokollari.

Shifrlash (dastlabki matnga o'girish) protokollari. Bu turdagi protokollarga ayrim simmetrik yoki asimmetrik shifrlash (dastlabki matnga o'girish) algoritmlarini kiritish mumkin. Shifrlash algoritmlari xabarlarni jo'natishda foydalaniladi. Natijada xabar ochiq matn ko'rinishidan shifrlangan ko'rinishga almashtiriladi.

Dastlabki matnga o'girish algoritmlari xabarni qabul qiluvchi tomonidan amalga oshiriladi va bu harakat natijasida shifrlangan xabar ochiq matn ko'rinishiga aylanadi. Xabarni maxfiyligi mana shu tarzda ta'minlanadi.

Uzatiladigan xabarlarni butunlik xossasini ta'minlash maqsadida simmetrik shifrlash (dastlabki matnga o'girish) algoritmlari odatda xabarlarni jo'natishda imitohimoyani qo'yish (IHQ) ni hisoblash algoritmlari bilan va xabarlarni qabul qilishda IHQ ni tekshirish algoritmlari bilan birgalikda foydalaniladi. Buning uchun shifrlash kalitlaridan foydalaniladi.

Asimmetrik shifrlash (dastlabki matnga o'girish) algoritmlaridan foydalanilganilib xabarlarni jo'natishda ERI ni hisoblash bilan va xabarlarni qabul qilishda ERIni tekshirish yo'li bilan xabarlarni butunlik xossasi ta'minlanadi.

Elektron raqamli imzo protokollari. Bu turdagi protokollar xabarlarni jo'natishda jo'natuvchining maxfiy kalitidan foydalanadi. ERIni hisoblashning qandaydir algoritmi va xabarni qabul qilishda o'zgartirishga yo'l qo'yilmaydigan, ma'lumotlar bazasida saqlanadigan jo'natuvchining ochiq kaliti yordamida ERIni tekshirishga asoslangan. Agar protokolni tekshirish jarayoni ijobiy yakun topsa, odatda qabul qilingan xabarni, uni ERIni va unga mos keluvchi ochiq kalitni arxivlash bilan bu jarayon tugallanadi. Agar ERI qabul qilingan xabarni faqatgina butunlik va

§1.4. Kriptografik protokol zaifligiga oid misollar

Kriptografik protokol zaifligiga misol sifatida Nidxem-Shreder protokolini keltirish mumkin. Ushbu protokol 1978 yilda yaratilgan bo'lib, bu protokol ikki ishtirokchi bir-birlarini o'zaro autentifikasiyalashga mo'ljallangan [3,10]. Bunda ishtirokchilar ochiq kalitli shifrlashdan foydalanishadi. 1995 yildagina G. Lowe tomonidan protokolning zaifligi aniqlandi, ungacha bu protokol mustahkam deb hisoblanilgan. Mavzuni bayon qilishda quyidagi belgilashlardan foydalaniladi:

a^+, b^+ - mos holda a va b ishtirokchilarning ochiq kalitlari;

r_a, r_b, r_c - mos holda a, b va c ishtirokchilar tomonidan tanlangan tasodifiy sonlar.

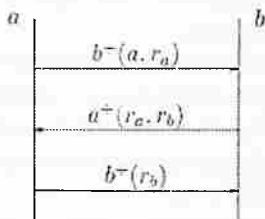
Nidxem-Shreder protokoli quyidagi harakatlardan iborat:

(1) $a \rightarrow b: b^+(a, r_a),$

(2) $a \leftarrow b: a^-(r_a, r_b),$

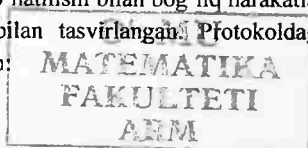
(3) $a \rightarrow b: b^+(r_b).$

Endi protokolni izohlash uchun uning 1.1-rasmda keltirilgan ko'rinishidan foydalanamiz.



1.1-rasm. Nidxem-Shreder protokolining sxematik ko'rinishi.

Kriptografik protokoldagi xabarni jo'natilishi bilan bog'liq harakatlar 1.1-rasmda alohida gorizontali strelka bilan tasvirlangan. Protokoldagi harakatlarni quyidagicha izohlash mumkin:



§1.3. Kriptografik protokollarni zaifligi

Raqiblar yoki buzg'unchilar harakatlari natijasida kriptografik protokolni ishlash jarayonida uning xavfsizlik xususiyatlari buzilishi mumkin.

Odatda raqiblar quyidagi 2 toifaga bo'linadi:

❖ passiv raqiblar. Ular protokol ishtirokchilari tomonidan uzatiladigan xabarlarini tutib olishlari va tahlil qilishlari mumkin;

❖ faol raqiblar. Ular passiv raqiblar qilgan ishlarni hamda quyida keltirilgan ishlarni amalga oshirishlari

- tutib olingan xabarlarini o'zgartirishlari yoki o'chirib tashlashlari,

- yangi xabarlarini shakllantirib, ularni protokol ishtirokchilariga jo'natishlari,

- o'zlarini protokol ishtirokchisi sifatida tutishi mumkin.

Bundan tashqari kriptografik protokol ishtirokchilari harakatlari (protokolda qabul qilingan harakatlarni tushunib yoki tushunmasdan buzishi) natijasida uni xavfsizlik xususiyatlari buzilishi mumkin.

Protokolni ishlash jarayonida uni xavfsizlik xususiyatlarini buzilish imkoniyati ushbu *kriptografik protokolning zaifligi deyiladi*.

Kriptografik protokol zaifligini bartaraf qilish yo'llarini izlashda raqib haqidagi quyidagi farazlardan foydalaniladi:

▪ raqib kriptografik protokolni to'liq biladi;

▪ kriptografik protokol ishtirokchilari jo'natadigan barcha xabarlarga ega bo'lish uchun raqibda yetarlicha imkoniyat mavjud. U xabarlarini o'zgartirishi va o'chirishi hamda boshqa xabarlar (o'ziniki) bilan almashtirishi mumkin;

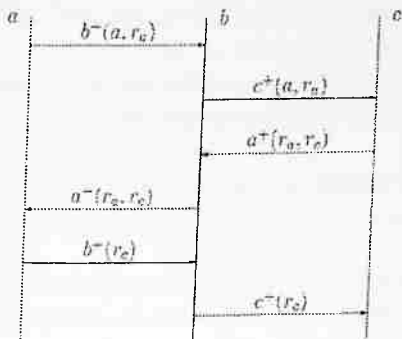
▪ agar raqib kalitlarni bilmasa, u holda u shifrlangan ma'lumotlardan unga mos keluvchi ochiq matn (dastlabki matni) ni tiklay olmaydi.

Protokolni mustahkamligi esa quyidagi faktorlar bilan xarakterlanadi:

- protokoldagi kriptografik mexanizmning ishonchliligi;

- protokolni to'g'ri amalga oshirilishi;

- protokoldagi harakatlarni ishtirokchilar tomonidan belgilangan ketma-ketlikda bajarilish aniqligi.



1.2-rasm. Ikki seansli Nidkem-Shreder protokoli.

▪ c ishtirokchi qabul qilingan $c^+(a, r_a)$ shifratni dastlabki matnga o'giradi. Hosil bo'lgan ochiq matn juftligi (a, r_a) ning birinchi elementi, ya'ni a ishtirokchining identifikatori asosida c ishtirokchi shifratni a ishtirokchi tomonidan jo'natilgan deb hisoblaydi.

▪ Nidkem-Shreder protokoliga asosan ikkinchi harakat sifatida c ishtirokchi r_c tasodifiy sonni generatsiya qilishi va $a^+(r_a, r_c)$ shifratni birinchi shifratni jo'natgan ishtirokchi (ya'ni, b ishtirokchi) ga jo'natadi (bunda u shifratni a ishtirokchiga jo'natayapman deb hisoblaydi).

▪ b ishtirokchi c ishtirokchidan qabul qilgan $a^+(r_a, r_c)$ shifratni a ishtirokchiga jo'natadi.

▪ a ishtirokchi b ishtirokchidan qabul qilgan $a^+(r_a, r_c)$ shifratni b ishtirokchi protokolning 2-chi qadamiga mos holda jo'natishi lozim bo'lgan xabar sifatida qabul qiladi, ya'ni shifratndan hosil qilgan r_c tasodifiy soniga b ishtirokchi tomonidan generatsiya qilingan son sifatida qaraydi.

▪ protokolni 3-qadamiga mos ravishda a ishtirokchi $b^-(r_c)$ shifratni b ishtirokchiga jo'natadi.

▪ b ishtirokchi esa qabul qilingan shifratndan r_c sonini hosil qiladi va protokol ikkinchi seansining uchinchi harakati sifatida

$$b \rightarrow c: c^-(r_c)$$

➤ birinchi harakat a ishtirokchining b ishtirokchiga $b^+(a, r_a)$ shifratni jo'natishdan iborat. Ushbu shifratga mos keluvchi ochiqmat a ishtirokchining identifikatori va u tomonidan tanlab olingan r_a tasodifiy son juftligi (a, r_a) dan tashkil topadi. $b^+(a, r_a)$ shifratni dastlabki matnga (a, r_a) o'girish natijasida b ishtirokchi a ishtirokchi tomonidan autentifikasiyalanadi.

➤ ikkinchi harakat b ishtirokchining a ishtirokchiga $a^-(r_a, r_b)$ shifratni jo'natishdan iborat. Bu shifratdan (r_a, r_b) juftlikni hosil qilgan a ishtirokchi haqiqatan ham jo'natuvchi b ekanligiga ishonch hosil qiladi. Chunki b dan boshqa hech kim r_a ni shifratdan hosil qilolmaydi. b ishtirokchini a ishtirokchiga r_b ni jo'natishdan maqsad a ishtirokchiga ham o'zining haqiqiylikini isbotlashga imkoniyat berishdir.

➤ uchinchi harakat a ishtirokchining b ishtirokchiga $b^-(r_b)$ shifratni jo'natishdan iborat. r_b ni hosil qilgan b ishtirokchi a ishtirokchining haqiqiylikiga ishonch hosil qiladi.

Shunday qilib, ushbu protokol muvaffaqiyatli tugagandan so'ng, a va b ishtirokchilar bir-birlarining haqiqiylikiga ishonch hosil qiladilar.

Ushbu protokolning kamchiliklaridan biri b ishtirokchi boshqalar bilan a ishtirokchi nomidan ish ko'rishi uchun o'zining kriptografik protokoldagi ishtirokchi statusidan foydalanishi bilan bog'liq. b ishtirokchi o'zining ishtirokchi statusidan foydalanib, a ishtirokchi nomidan ish ko'rishi 1.2-rasmida keltirilgan.

1.2-rasmni Nidexem-Shreder protokoli ikki seansini bajarilishini tasvirlovchi 2 ta diagrammani birlashmasi sifatida qabul qilish mumkin:

- birinchi seansda a va b ishtirokchilar qatnashadi;
- ikkinchi seansda b va c ishtirokchilar qatnashadi.

Seanslar bajarilishi jarayonida a , b va c ishtirokchilar harakatlarini diagrammalar asosida quyidagicha izohlash mumkin:

▪ a va b ishtirokchilar birinchi seansning birinchi harakatini amalga oshirgandan so'ng, b ishtirokchi qabul qilgan $b^-(a, r_a)$ shifratdan (a, r_a) juftlikni dastlabki matnga o'giradi. Undan foydalanib, $c^-(a, r_a)$ shifratni hosil qiladi. Bu shifratni b ishtirokchi a ishtirokchi nomidan ikkinchi seansning birinchi harakati sifatida c ishtirokchiga jo'natadi.

Ushbu hujum turi kalitlarni uzatish protokollarida ilgari ishlatilgan seans kalitidan takroran foydalanish uchun ko'p qo'llaniladi. Seansni butunligini ta'minlash va unga ortiqcha xabarlar kiritilishiga yo'l qo'ymaslik mazkur hujumni bartaraf qilish usullari asosini tashkil qiladi. Buning uchun quyidagilardan foydalaniladi:

- «savol-javob» mexanizmi;
- uzatilayotgan xabarlarga vaqt nishoni yoki tasodifiy sonlarni qo'shish.

3. *Akslantirishga asoslangan hujum (reflection attack)*. Ushbu hujum ilgari uzatilgan xabarni jo'natuvchining o'ziga uzatishdan iborat. Ko'pchilik hollarda ushbu hujum turi xabardan takroran foydalanish hujumlari turkumiga kiritiladi. Ushbu hujumdan saqlanish uchun protokollar nosimmetrik tarzda quriladi, ya'ni protokol qadamlari shunday o'zgartiriladiki, natijada ishtirokchilar turli harakatlarni bajaradilar. Shuningdek, shifrlangan xabarlarga ishtirokchilar identifikatorlarini qo'shish yoki xabarlarni qabul qilish va uzatishda turli kalitlardan foydalanishadi.

4. *Xabarni uzatishni kechiktirish (forced delay)*. Bunda xabardan keyinroq foydalanish maqsadida xabar raqib tomonidan ushlab qolinadi. Bu hujum ham xabardan takroran foydalanish hujumlari turkumiga tegishli. Tasodifiy sonlar bilan birgalikda javob berish oralig'ini cheklash va vaqt nishonidan foydalanish ushbu hujumni bartaraf qilish imkonini beradi.

5. *Kombinasiyalashgan hujum (interleaving attack)*. Bu hujum turi ilgari bajarilgan protokollar ma'lumotlarini kombinasiyasidan foydalanish asosida aldashga asoslangan. Protokollar seanslari va alohida xabarlarni butunligini ta'minlash ushbu turdagi hujumlarni oldini olishga yordam beradi.

6. *Parallel seansli hujum (parallel-session attack)*. Bu hujum bundan oldin keltirilgan hujumning xususiy holi bo'lib, unda bitta seansdagi xabardan boshqa ishtirokchi bilan bo'ladigan seansda foydalanish uchun raqib bir vaqtning o'zida bir necha parallel seanslar tashkil qiladi. Bundan oldingi §1.4. da keltirilgan Nidkem-Shreder protokolida ikkinchi seansning tashkil qilinishi ushbu hujumga misol bo'ladi.

harakatni amalga oshiradi, ya'ni $c^+(r_c)$ shifmatni c ishtirokchiga jo'natadi.

Bu harakatdan so'ng, c ishtirokchi protokolning ushbu seansini a ishtirokchi bilan bajarganligiga ishonch hosil qiladi (bu esa noto'g'ri).

§1.5. Kriptografik protokollarga nisbatan keng tarqalgan hujum turlari

Protokoldagi xabarlarini tahlil qilish hamda protokol ishini buzish uchun protokolda ko'zda tutilmagan harakatlarni bajarish va protokol ishtirokchilariga tegishli bo'lgan maxfiy axborotlarga ega bo'lish maqsadida qilingan urinishlar *protokolga qilingan hujum deyiladi*.

Agarda protokolni xavfsizligini ta'minlovchi xususiyatlaridan biri buzilsa, protokolga qilingan *hujum muvaffaqiyatli deyiladi*.

Protokolga qilinadigan hujumlar protokolni tahlil qilishning turli usullariga asoslangan bo'ladi.

Hozirgi kunda kriptografik protokollarga nisbatan keng tarqalgan hujum turlari quyidagilardan iborat:

1. *Almashtirish (impersonation)*. Bu hujum asosini bir foydalanuvchini boshqasi bilan almashtirish uchun urinish tashkil qiladi. Buzg'unchi boshqa bir ishtirokchi nomidan ish ko'rib, uning harakatlarini to'liq imitasiya qiladi. Natijada protokolning ayrim qadamlarini qalbakilashtirish uchun ma'lum bir formatdagi xabarlarga ega bo'ladi.

Ushbu hujumga qarshilik ko'rsatish uchun quyidagi usullardan foydalanish mumkin:

- identifikasiyalash algoritmiga oid axborotni raqibdan sir tutish;
- protokolning turli qadamlarida uzatiladigan xabarlar uchun har xil formatlardan foydalanish;
- xabarlarga identifikasiya nishoni va uning tartib nomerini kiritish.

Uchinchi tomon (ishonchli server) ishtirokidagi protokollarda serveni almashtirishga asoslangan hujumlar bo'lishi mumkin.

2. *Xabardan takroran foydalanish (replay attack)*. Joriy yoki undan oldingi seansdagi oldin uzatilgan xabardan yoki uning qandaydir qismidan protokolning joriy seansida takroran foydalanish ushbu hujumning asosiy g'oyasidir.

$$(1) A \rightarrow C(B): E_{k_A}(k),$$

$$(2) A \leftarrow C(B): E_{k_A}(k),$$

$$(3) A \rightarrow C(B): k.$$

Bu yerda ham C raqib B ishtirokchi nomidan ish ko'rmoqda. U A ishtirokchining birinchi xabarini uning o'ziga jo'natdi. A ishtirokchi qabul qilingan shifratni tekshirib o'tirmasdan, o'zi bilmagan holda dastlabki matnga o'girdi. Natijada o'zi tomonidan generatsiya qilingan maxfiy kalit k ni hosil qildi. Ushbu kalitni C raqibga jo'natdi va bu kalit tarmoqda ochiq holda paydo bo'ldi.

3-chi hujum - kombinasionalashgan hujum (interleaving attack).

$$(1) A \rightarrow C(B): E_{k_A}(k),$$

$$(1') A \rightarrow C(B): E_{k_A}(k'),$$

$$(2') A \leftarrow C(B): E_{k_A}(k),$$

$$(3') A \rightarrow C(B): k,$$

$$(2) A \leftarrow C(B): M,$$

$$(3) A \rightarrow C(B): D_{k_A}(M).$$

Bu yerda M - ixtiyoriy ahamiyatsiz xabar. Ushbu hujumda xabarni uzatishni kechiktirish (*forced delay*) va xabardan takroran foydalanish (*reply attack*) usullarining kombinasiasidan foydalanilgan.

§2.2. Diffi–Xellman protokoli

Ushbu protokol umumiy maxfiy kalit hosil qilish uchun ishlatiladi. Protokolning mustahkamligi diskret logarifmlash masalasining murakkabligi bilan xarakterlanadi. Bu protokol «o'rtadagi odam» hujumiga nisbatan zaif va undan himoyalaniish uchun har bir ishtirokchi o'zlarining har bir xabarlariga elektron imzo qo'yishlari lozim bo'ladi.

Protokolni amalga oshirishdan oldin ishtirokchilar p – katta tub soni hamda $Z_p^* = \{1, p-1\}$ multiplikativ guruh elementi α haqida kelishib oladilar. Ishtirokchilar umumiy maxfiy kalit k ni hosil qilish uchun x va y

2-BOB. KRIPTOGRAFIK PROTOKOLLAR VA ULARNING XAVFSIZLIGIGA QILINADIGAN ASOSIY HUJUMLAR

Ushbu bobda ayrim kriptografik protokollarni zaifliklari va ular asosida qilinadigan hujumlar keltiriladi.

§2.1. Shamir–Rivest–Adleman protokoli

Bu protokol asosida qandaydir umumiy bo'lgan maxfiy axborotdan foydalanmasdan, A ishtirokchi B ishtirokchiga maxfiy k kalitni uzatadi. Quyida protokol sxematik ko'rinishda keltirilgan.

$$(1) A \rightarrow B: E_{k_A}(k),$$

$$(2) A \leftarrow B: E_{k_B}(E_{k_A}(k)),$$

$$(3) A \rightarrow B: D_{k_A}(E_{k_B}(E_{k_A}(k))) = E_{k_B}(k).$$

Bu yerda k_A , k_B - mos holda A va B ishtirokchilarning maxfiy kalitlari, E shifrlash almashtirishi esa quyidagi xususiyatga ega:

$$E_{k_1}(E_{k_2}(x)) = E_{k_2}(E_{k_1}(x)).$$

1-chi zaiflik. Ishtirokchilarni autentifikasiyalashning yo'qligi. Shu sababli ishtirokchini almashtirib qo'yish yo'li bilan hujum qilish mumkin.

1-chi hujum – almashtirish (impersonation attack).

$$(1) A \rightarrow C(B): E_{k_A}(k),$$

$$(2) A \leftarrow C(B): E_{k_C}(E_{k_A}(k)),$$

$$(3) A \rightarrow C(B): D_{k_A}(E_{k_C}(E_{k_A}(k))) = E_{k_C}(k).$$

Bu yerda k_C - C raqibning maxfiy kaliti.

C raqib B ishtirokchi nomidan ish ko'rib, unga kelayotgan xabarlarni blokirovka qilmoqda. Natijada B ishtirokchi nomidan ish ko'rish va A ishtirokchi bilan axborot almashish uchun undan maxfiy kalit k ni oldi.

2-chi zaiflik. Ishtirokchilar xabarlari simmetrik, ya'ni ular bir xil harakatlarni bajarmoqdalar. Shu bois, xabardan takroran foydalanish (replay attack) mumkin.

2-chi hujum - xabardan takroran foydalanish (replay attack).

protokolidagi «oʻrtadagi odam» hujum usuliga nisbatan zaiflikni bartaraf qilish maqsadida ishlab chiqilgan.

MTI/protokolining MTI/A0 varianti.

Faraz qilaylik, A va B ishtirokchilar $1 \leq a, b \leq p-2$ shart asosida oʻzlarining maxfiy kalitlari a va b sonlarini tasodifiy ravishda generatsiya qilishgan. Ularning ushbu maxfiy kalitlarga mos $\beta_A = \alpha^a \bmod p$ va $\beta_B = \alpha^b \bmod p$ ochiq kalitlari ham mavjud. Ishtirokchilar umumiy maxfiy kalit k ni hosil qilish uchun $1 \leq x, y \leq p-2$ shart asosida x va y tasodifiy sonlarini generatsiya qilishlari kerak. Undan soʻng bevosita protokolni quyidagi tarzda amalga oshiradilar:

$$A \rightarrow B: \alpha^x \bmod p,$$

$$A \leftarrow B: \alpha^y \bmod p.$$

Endi, ishtirokchilar umumiy maxfiy kalit $k = \alpha^{xb-ya} \bmod p$ ni

$$k_A = (\alpha^x)^y \beta_B^y \bmod p, k_B = (\alpha^y)^x \beta_A^x \bmod p$$

ekvivalent formulalar bilan hisoblaydilar.

Bu protokoldagi ixtiyoriy xabarni almashtirish (oʻzgartirish) natijasida ishtirokchilar turli kalitlarga ega boʻladi. Bu esa buzgʻunchini barcha xabarlarini oʻqish imkonidan mahrum qiladi. Ushbu holatni «oʻrtadagi odam» hujum usuliga nisbatan protokol kalitlarini autentifikatsiyasi xossalari buzilmaganligi bilan izohlash mumkin.

Shu bilan birgalikda ushbu protokolda ishtirokchilarni autentifikatsiyalash va kalitlarni toʻgʻri qabul qilinganligini tasdiqlash eʼtiborga olinmagan. Bu esa protokolni zaifligini anglatadi. Protokolni mustahkamligini oshirish maqsadida xabarlariga ishtirokchining sertifikatini qoʻshib joʻnatish ham uzatilayotgan xabarlar mazmunini oʻzgartirishga boʻlgan urinishlarni bartaraf qilolmaydi hamda ishtirokchilarni autentifikatsiyalashni taʼminlay olmaydi.

MTI/A0 protokoliga hujum. Bunda C buzgʻunchi A ishtirokchining sertifikatini oʻziniki bilan almashtirib qoʻyadi. Faraz qilaylik, A ishtirokchi quyida keltirilgan sertifikatga ega boʻlsin

$$\text{cert}_A = (A, \beta_A, \text{Sig}_T(A, \beta_A)).$$

tasodifiy sonlarni $1 \leq x, y \leq p-2$ shart asosida generatsiya qilishlari lozim bo'ladi. Undan so'ng bevosita protokolni quyidagi tarzda amalga oshiradilar:

$$A \rightarrow B: \alpha^x \bmod p,$$

$$A \leftarrow B: \alpha^y \bmod p.$$

Umumiy maxfiy kalit k

$$k = (\alpha^y)^x = (\alpha^x)^y \bmod p$$

formula bilan hisoblanadi.

Zaifligi: ishtirokchilarni autentifikatsiyalashning yo'qligi.

Hujum: «o'rtadagi odam».

$$A \rightarrow C(B): \alpha^x \bmod p,$$

$$C(A) \rightarrow B: \alpha^{x^*} \bmod p,$$

$$C(A) \leftarrow B: \alpha^y \bmod p,$$

$$A \leftarrow C(B): \alpha^{y^*} \bmod p.$$

Bu yerda C ishtirokchi A ishtirokchi nomidan B ishtirokchi bilan aloqa o'rnatishga urinmoqda. Buning uchun C ishtirokchi aloqa qilishdan oldin x^* va y^* tasodifiy sonlarni $1 \leq x, y \leq p-2$ shart asosida generatsiya qilib olgan. U aloqa qilish vaqtida α^x va α^y miqdorlarni mos holda α^{x^*} va α^{y^*} miqdorlar bilan almashtirib qo'yadi. Natijada C ishtirokchi bilan aloqa o'rnatish uchun A ishtirokchi bilan $k_{AC} = (\alpha^x)^{y^*} \bmod p$, B ishtirokchi bilan $k_{CB} = (\alpha^{y^*})^{x^*} \bmod p$ umumiy kalitga ega bo'ladi. Axiyri C nazorat qilishga erishadi. Afsuski, A va B ishtirokchilar buni sezmaydilar. Ular bir-birlari bilan aloqa qilmoqdamiz deb hisoblaydilar.

§2.3. Masumoto-Takashima-Imai (MTI) protokoli

Ushbu protokol T.Masumoto, I.Takashima va X.Imailar tomonidan 1986 yilda taklif qilingan [3,10]. MTI protokoli Diffi-Xellman

olingan [3,10]. Protokolni sxematik ko'rinishda quyidagicha ifodalash mumkin:

$$A \rightarrow B: A, B, m_A = \alpha^x \bmod p,$$

$$A \leftarrow B: B, A, m_B = \alpha^y \bmod p, E_k(\text{Sig}_B(m_B, m_A)),$$

$$A \rightarrow B: A, B, E_k(\text{Sig}_A(m_A, m_B)).$$

Bu yerda Sig_A va $\text{Sig}_B - k = \alpha^{xy} \bmod p$ umumiy kalitga mos keluvchi A va B ishtirokchilarning mos holda raqamli imzolari.

Protokolning 2-chi va 3-chi qadamlarida raqamli imzolardan foydalanish, qabul qilingan xabarni aynan xabar qabul qilingan ishtirokchidan olinganligini kafolatlaydi. Umumiy kalit qiymatini to'g'ri hisoblanganligini o'zaro tasdiqlashni ta'minlash maqsadida protokolda ishtirokchilar elektron raqamli imzolari qiymatlarini simmetrik algoritim bilan shifrlash ham qo'lanilgan. Chunki, noto'g'ri hisoblangan kalit bilan elektron raqamli imzolar qiymatlarini to'g'ri hisoblash mumkin emas.

Noma'lum umumiy kalit asosida hujum (unknown key-share attack, UKS attack). Ushbu hujum 1996 yilda G.Lowe tomonidan ishlab chiqilgan, uni sxematik ko'rinishda quyidagicha ifodalash mumkin:

$$A \rightarrow C(B): A, B, m_A,$$

$$C \rightarrow B: C, B, m_A,$$

$$C \leftarrow B: B, C, m_B, E_k(\text{Sig}_B(m_B, m_A)),$$

$$A \leftarrow C(B): B, A, m_B, E_k(\text{Sig}_B(m_B, m_A)),$$

$$A \rightarrow C(B): A, B, E_k(\text{Sig}_A(m_A, m_B)).$$

C buzg'unchi o'zi va B ishtirokchi o'rtasidagi qonuniy xabar almashinuvidan foydalanib, A ishtirokchiga hujum tashkil qilishni mo'ljallagan. Natijada u o'zini B ishtirokchi ekanligiga A ishtirokchini ishontirishi mumkin. C buzg'unchi A ishtirokchini maxfiy kalitini bilmasligi bois, u B ishtirokchiga to'g'ri javob berolmaydi. Shunga qaramasdan, u qandaydir javobni jo'natadigan bo'lsa, B ishtirokchi bu javobni rad qilishi mumkin. Shu sababli uning B ishtirokchi bilan boshlangan seansi tugallanmagan.

A ishtirokchidan B ishtirokchiga jo'natilgan xabarlarni $k = \alpha^{xy}$ kalitni C buzg'unchi bilmasligi oqibatida o'qiy olmaydi. Shu bois, bu

C buzg'unchi ham o'zi uchun kalitlarni qayd qilish markazidan

$$cert_C = (C, \beta_A^e, Sig_T(C, \beta_A^e))$$

sertifikatni olsin. Bu yerda e soni A ishtirokchini kalitidan foydalanishni yashirishga mo'ljallangan ixtiyoriy son. Protokol quyidagi tarzda amalga oshiriladi:

$$A \rightarrow C(B): cert_A, \alpha^x \bmod p,$$

$$C \rightarrow B: cert_C, \alpha^x \bmod p,$$

$$C \leftarrow B: cert_B, \alpha^y \bmod p,$$

$$A \leftarrow C(B): cert_B, (\alpha^y)^e \bmod p.$$

Bu yerda C buzg'unchi B ishtirokchiga keladigan xabarlarni blokirovka qilish imkoniga ega. U bitta seansdagi xabardan boshqa ishtirokchi bilan bo'ladigan seansda foydalanish maqsadida bir vaqtning o'zida 2 ta parallel seanslar tashkil qilgan. Natijada B ishtirokchi xabar almashish uchun

$$k = \alpha^{bx+ay} \bmod p$$

maxfiy kalitga ega bo'ldi. Lekin, u bu kalitni C buzg'unchi bilan (A ishtirokchi bilan emas) umumiy deb hisoblaydi. Ushbu kalit A ishtirokchida ham mavjud. Shu sababli bu kalit bilan A ishtirokchi tomonidan shifrlangan va jo'natilgan xabarni B ishtirokchi C ishtirokchidan qabul qilingan deb hisoblaydi.

Demak, ushbu protokol A ishtirokchi uchun kalitni autentifikasiyalashni ta'minlasada, ammo B ishtirokchi uchun kalitni autentifikasiyalashni ta'minlamaydi. Shuningdek, ishtirokchilar autentifikasiyalanmaydi.

§2.4. STS protokoli

STS (station-to-station) protokoli U.Diffi (W. Diffie), P.Van Oorshot (P. Van Oorschot) va M.Veyner (M. Wiener) lar tomonidan 1992 yilda yilda taklif qilingan. Bu protokol Diffi–Xellman protokoli asosida yaratilgan bo'lib, unda ishtirokchilarni autentifikasiyalanishi e'tiborga

3-BOB. AUTENTIFIKASIYALASH VA IDENTIFIKASIYALASH PROTOKOLLARI

Ma'lumki, autentifikasiyalash protokollari autentifikasiya masalalarini yechish uchun mo'ljallangan [3,9,10]. Ushbu protokollar vositasida kalitlar, xabarlar, xabarlarini yaratilish vaqtlari va h.k. larni haqiqiyliги isbotlanadi. Axborot tizimidagi foydalanuvchi yoki axborot almashinuvida ishtirok etuvchilarni autentifikasiyalash masalalari katta ahamiyat kasb etadi. Masalan, xavfsizligi katta qiziqishga ega bo'lgan resurslar (bank hisob raqamlari, maxfiy ma'lumotlar bazasi, muhim strategik ahamiyatga ega bo'lgan binolar va boshqalar) ga kirish va ulardan foydalanishni xohlovchi barcha foydalanuvchilarni autentifikasiyalash va identifikasiyalash ushbu resurslarni xavfsizligini ta'minlashda muhim o'rin egallaydi.

Autentifikasiyalash sxemalarining mustahkamligiga qo'yiladi-gan talablar nol oshkoralik bilan isbotlash tushunchasi asosida shakllantiriladi. Shu sababli nol oshkoralikka asoslangan barcha protokollar autentifikasiyalash sxemalari sifatida ishlatilishi mumkin. Ammo, asosiy muammo ularning samaradorligi bilan bog'liq. Chunki, bu protokollarning ko'pchiligi katta uzunlikka ega bo'lgan yopiq kalit, katta sondagi raundlar, yuqori murakkabliklarga ega bo'lgan hisoblashlardan foydalanishni talab etadi. Shuningdek, bu protokollarni mustahkamligini isbotlash katta qiyinchilik bilan bajariladi.

Protokollarning nol oshkoralik xossalarini isbotlash masalasi, umuman olganda notrivial masala hisoblanadi. Oshkoraligi nol bo'lgan deb nomlanuvchi ko'pgina protokollar matematik ma'noda absolyut nol oshkoralikka ega emas. Ammo, bu faktor ko'p hollarda asosiy hal qiliuvchi ko'rsatkich sifatida e'tirof etilmaydi.

Yuqorida keltirilgan sabablarga ko'ra, autentifikasiyalash va identifikasiyalash sxemalarini ishlab chiquvchilar asosiy e'tiborni ularning samaradorligiga qaratishadi.

Autentifikasiyalash va identifikasiyalash sxemalarining to'liqligi ushbu protokollarning konstruksiyasidan kelib chiqadi. Bu sxemalarning korrektiligi esa katta qiyinchiliklar bilan isbotlanadi. Shu bois, ko'pgina autentifikasiyalash va identifikasiyalash sxemalarining korrektiligi

hujum aslida unchalik xavfli emas. Lekin, A ishtirokchi C buzg'unchini B ishtirokchi sifatida qabul qilishga ishontirgan.

Shunday qilib, protokol ishtirokchilarini va B ishtirokchi uchun kalitni autentifikatsiyalanishi ushbu protokolda ta'minlanmagan. Natijada B ishtirokchi umumiy kalitni A ishtirokchi bilan emas, balki C ishtirokchi bilan shakllantirdim deb hisoblaydi.

Modifikatsiyalangan STS protokoli.

K.Boyd va A.Maturalar tomonidan 2004 yilda taklif qilingan, modifikatsiyalangan STS protokolini quyidagi sxematik ko'rinishda keltirish mumkin:

$$A \rightarrow B: A, B, m_A = \alpha^x \text{ mod } p,$$

$$A \leftarrow B: B, A, m_B = \alpha^y \text{ mod } p, \text{Sig}_B(m_B, m_A), h_{k_0}(m_B, m_A),$$

$$A \rightarrow B: A, B, \text{Sig}_A(m_A, m_B), h_{k_0}(m_A, m_B).$$

Bu yerda $k_0 = f(k) - h$ xesh funksiyaning kalitli parametri bo'lib, u $k = \alpha^{xy} \text{ mod } p$ seans kalitini qandaydir funksiyasining qiymati sifatida aniqlanadi.

Noma'lum umumiy kalit asosida ikkitomonlama hujum (bilateral unknown key-share attack, BUKS attack). Ushbu hujumni quyidagi sxematik ko'rinishda keltirish mumkin:

$$A \rightarrow C: A, B, m_A,$$

$$C \rightarrow D: A, B, m_A,$$

$$D \rightarrow B: D, B, m_A,$$

$$D \leftarrow B: B, D, m_B, \text{Sig}_B(m_B, m_A), h_{k_0}(m_B, m_A),$$

$$C \leftarrow D: B, A, m_B, h_{k_0}(m_B, m_A),$$

$$A \leftarrow C: C, A, m_B, \text{Sig}_C(m_B, m_A), h_{k_0}(m_B, m_A),$$

$$A \rightarrow C: A, C, \text{Sig}_A(m_A, m_B), h_{k_0}(m_A, m_B),$$

$$C \rightarrow D: A, B, h_{k_0}(m_A, m_B),$$

$$D \rightarrow B: D, B, \text{Sig}_D(m_A, m_B), h_{k_0}(m_A, m_B).$$

C va D ishtirokchilarning qallobligi natijasida umumiy kalit hosil qilishgan A va B ishtirokchilar boshi berk ko'chaga kirib qolishadi. Natijada A ishtirokchi C ishtirokchi bilan, B ishtirokchi D ishtirokchi bilan umumiy kalit hosil qilganligiga ishonadi.

mavjud bo'lgan. Insonlar u paytlarda bu masalani yechishda og'zaki parollar, qandaydir belgilar yoki murakkab muhrlar kabi soddaroq ob'ektlardan foydalanishgan. Mexanik qurilmalarning paydo bo'lishi va ulardan foydalanishga asoslangan autentifikasiyalash usullari haqiqiylikni tekshirishni sezilarli darajada osonlashtirdi. XX asrda axborot texnologiyalarining gurkirab rivojlanishi autentifikasiyalash prosedurasini yanada osonlashtirdi.

Autentifikasiyalash tizimi elementlari. Ixtiyoriy autentifikasiya-lash tizimi quyidagi elementlardan tashkil topgan bo'ladi:

Sub'ekt - bu autentifikasiyalash prosedurasi o'tkaziladigan ob'ekt.

Sub'ektning xarakteristikasi – shu sub'ektga xos bo'lgan uning alohida belgilari.

Autentifikasiyalash tizimining xo'jayini yoki egasi autentifikasiyalash tizimining ishlash prinsipi va mexanizmi, autentifikasiyalash prosedurasini o'tkazish va uni nazorat qilishga javobgar bo'lib, sub'ektga ma'lum bir huquqlar berishi yoki uni huquqlaridan mahrum qilishi mumkin.

Autentifikasiyalash mexanizmi – autentifikasiyalash tizimining ishlash prinsipi.

Mexanizm sub'ektga ma'lum bir huquqlar berishi yoki uni huquqlaridan mahrum qilishi mumkin.

Autentifikasiyalash tizimining elementlariga quyidagicha misol keltirish mumkin. «Ali bobo va qirq qaroqchi» ertagini eslaydigan bo'lsak, unda sub'ekt sifatida parolni biluvchi odam, bankomat tizimida esa bank kartasining egasi sub'ekt sifatida ta'riflanishi mumkin. Sub'ektning xarakteristikasi sifatida mos holda «Sezam, ochilgil» yoki maxfiy parol, yoki bank kartasi va shaxsiy identifikator xizmat qiladi. Qirq qaroqchilar va autentifikasiyalash tizimiga ega bo'lgan korxonalar, ya'ni bank autentifikasiyalash tizimining xo'jayini maqomida foydalaniladi.

Autentifikasiyalash mexanizmi sifatida ma'lum bir so'zga reaksiya bildiruvchi – sehrli qurol yoki qurilma va parolni tekshiruvchi programma ta'minoti yoki bank kartasi va sub'ekt identifikatorini tekshiruvchi programma ta'minoti bo'lishi mumkin.

Ruxsatni boshqarish mexanizmi sifatida – qirq qaroqchilar g'origa kirishdagi toshni siljituvchi mexanizm yoki bankdagi registrasiya jarayoni yoki bank amallarini bajarishga berilgan ruxsatnomani ko'rsatish mumkin.

hanuzgacha isbotlanmagan. Lekin, shunday bo'lsa-da bu turdagi protokollar yuqori samaradorlik bilan amaliyotga keng qo'llanilmoqda. Buning natijasida axborot xavfsizligida yaxshi natijalarga erishilmoqda.

Ushbu bobda autentifikasiyalash va identifikasiyalashning asosiy tushunchalari, autentifikasiyalash usullari, autentifikasiyalash protokollari turlari, *parol* bo'yicha autentifikasiyalashga qilinadigan hujumlar va ularni bartaraf qilish, simmetrik va asimmetrik kriptosxemalardan foydalanuvchi protokollar, «savol-javob» turidagi autentifikasiyalash protokollari haqida ma'lumotlar bayon qilingan.

Shuni alohida qayd etish lozimki, bu bobda axborot resurslarini noqonuniy foydalanuvchilardan himoyalash masalalarida hozirgi kunda amaliyotda keng qo'llanilayotgan, yuqori samaradorlikka ega bo'lgan autentifikasiyalash va identifikasiyalash sxemalari keltirilgan.

§3.1. Autentifikasiyalash va identifikasiyalashning asosiy tushunchalari

Quyida keltiriladigan tushunchalar axborot texnologiyalari va axborot xavfsizligida keng uchraydi. Shu sababli ularga izoh berib o'tish maqsadga muvofiq hisoblanadi.

Foydalanuvchi, shuningdek, qurilmaviy-dastur komponenti yoki foydalanuvchi nomidan ish ko'ruvchi jarayonlar *sub'ekt* deb nomlanadi.

Autentifikasiyalash (ingl. authentication) tizimga kiruvchi sub'ektni uning taqdim qilgan identifikatori asosida haqiqiylikni tekshirish prosedurasi hisoblanadi. Masalan, foydalanuvchi kiritgan *parolni* ma'lumotlar bazasidagi *parol* bilan taqqoslash orqali foydalanuvchini haqiqiylikni tekshirish, elektron xatni jo'natuvchini shifrlash kaliti orqali elektron raqamli imzoni haqiqiylikni tekshirish va h.k. Ushbu atama rus tilida asosan axborot texnologiyalari sohasida ishlatiladi.

Identifikasiyalash autentifikasiyalashning xususiy holi bo'lib, u sub'ektni belgilari (identifikatori) ga asosan sub'ektni o'zi ekanligini tekshirish prosedurasidir.

Qadimgi vaqtlardan buyon insoniyat oldida muhim xabarlarini haqiqiylikni tekshirish va tasdiqlash masalasi kabi murakkab masala

joylashtiriladi, masalan, plastik karta yoki smart kartada. Buzg'unchi uchun parolni buzishga nisbatan bunday qurilmani qo'lga kiritish katta muammolar keltirib chiqaradi, bunday qurilmalar yo'qotilgan paytda sub'ekt kerakli joylarga xabar berishi mumkin. Bu usul esa parolli mexanizmga nisbatan tizimni yuqoriroq darajada himoyalaydi, ammo uni qo'llash katta mablag' talab qiladi. Autentifikasiyalashning ushbu faktori axborotni kriptografik akslantiruvchi qandaydir fizik qurilmaga «sub'ekt ega» prinsipiga asoslangan.

Biometrika. Sub'ektning jismoniy belgilaridan uning xarakteristikasi sifatida foydalanish mumkin. Biometrika sifatida sub'ektning portreti, qo'l panjasi yoki kafti izi, tovushi hamda ko'zining alohida belgilaridan foydalanish mumkin. Ushbu usul yuqoridagi usullarga nisbatan anchagina soddaroq: parolni yodda saqlashga, o'zi bilan birga autentifikasiya qilmasini olib yurishga hojat qolmaydi. Ammo, biometrik parametrlari o'xshash bo'lgan buzg'unchini rad qilish yoki haqiqiy sub'ektni tanishi uchun biometrik tizim yuqori sezgirlikka ega bo'lishi lozim. Shu bilan birgalikda biometrik tizimni narxi nisbatan ancha baland. Mana shu kabi kamchiliklariga qaramasdan ushbu tizim istiqbolli faktor sifatida qaralmoqda. Autentifikasiyalashning ushbu faktori «sub'ekt qandaydir biometrik belgilarga ega» prinsipiga asoslangan.

Autentifikasiyalash jarayonida autentifikasiyalashning faqatgina bitta usulidan foydalanilsa, *bir faktorli autentifikasiyalash*, agar bir necha usulidan foydalanilsa *ko'pfaktorli autentifikasiyalash deyiladi*.

Kriptografik vositalar asosida identifikasiyalash uchun yuqorida keltirilgan 3 ta autentifikasiyalash usuli sub'ektni qandaydir axborotga ega ekanligiga asoslangan bitta autentifikasiyalashga keltirilishi mumkin. Haqiqatan ham, fizik qurilmalardagi axborotlar yoki biometrik ma'lumotlar sub'ektni bir qiymatli aniqlaydigan qandaydir kalit (kriptografik tizimlar yoki protokollar asosida identifikasiyalashda) yoki parol (parolli sxemalar yordamida identifikasiyalash va autentifikasiyalashda) ga almashtirilishi mumkin.

Oxirgi vaqtlarda kengaytirilgan yoki ko'pfaktorli deb nomlanuvchi autentifikasiyalash keng qo'llanilmoqda. Autentifikasiyalashning ushbu usuli bir necha faktorlaridan birgalikda foydalanishga asoslanganligi sababli u o'z navbatida tizimning himoyalanganlik darajasini kuchaytiradi.

Autentifikasiyalash faktorlari. Hattoki, kompyuterlar paydo bo'lmagan davrlarda ham sub'ektni xarakterlovchi belgilardan, xarakteristikalaridan amaliyotda foydalanib kelingan. Hozirgi kunda u yoki bu xarakteristikalaridan autentifikasiyalash tizimida foydalanish talab qilinadigan ishonchlilikka, himoyalanganlikka va joriy qilish narxi bilan belgilanadi.

Autentifikasiyalash jarayonida sub'ekt tomonidan autentifikasiyalash tizimiga taqdim qilinadigan ma'lum bir turdagi axborot *autentifikasiyalash faktori* deyiladi.

Autentifikasiyalashning quyidagi 3 ta faktorini ko'rsatish mumkin.

Parol. Parol – bu faqat unga ruxsati bo'lgan sub'ektgina bilishi mumkin bo'lgan maxfiy axborotdir. Parol sifatida og'zaki so'z, matnli so'z, qulflar uchun raqamlar kombinatsiyasi yoki shaxsiy identifikatsiya nomeri (PIN) dan foydalanish mumkin. Parolli mexanizmi nisbatan oson qo'llash mumkin, Shuningdek, uni joriy qilish katta mablag' talab etmaydi. Shu bilan birgalikda bu mexanizm sezilarli kamchiliklardan ham xoli emas. Parolni maxfiy saqlash ko'p hollarda muammolar keltirib chiqaradi, buzg'unchilar doimo parolni o'g'irlashni, buzishni har xil yo'llarini o'ylab topadilar. Bu esa parolli mexanizmi himoyasini zaiflashtiradi.

Parolli sxemalar odatda kompyuter tizimida qayd qilingan foydalanuvchilarni autentifikatsiya qilish uchun ishlatiladi. Bunday sxemalarni ishlatish uchun tizimda qayd qilingan foydalanuvchilarni identifikatorlari va parollari kompyuter tizimida saqlangan bo'lishi lozim. Albatta, kompyuter tizimida parollarni ochiq holda saqlash maqsadga muvofiq emas, shu sababli ular ustida bajarilgan matematik almashtirishlar natijasi sifatida, ya'ni shifrlangan yoki xeshlangan ko'rinishda saqlanadi.

Autentifikasiyalashning ushbu faktori «sub'ekt biladi» prinsipi asosida amalga oshiriladi. Unga ko'ra kompyuter tizimining boshqa ob'ektlariga noma'lum bo'lgan qandaydir axborot (parol, shaxsiy identifikatsiya nomeri, maxfiy kalit) ni sub'ekt biladi. Ushbu axborotni sub'ekt «savol-javob» protokollarida namoyish qiladi.

Autentifikasiyalash qurilmasi. Bu qurilma sifatida shaxsiy muhr, qulfnig kaliti, kompyuterlar uchun sub'ektning xarakteristikasini saqlovchi ma'lumotlar fayli, parollar hosil qiluvchi generator qo'llanilishi mumkin. Sub'ekt xarakteristikasi ko'p hollarda maxsus qurilmalarga

Sub'ekt tomonidan kiritilgan parol kompyuter tarmog'i orqali ikki xil usulda uzatilishi mumkin:

a) shifrlanmasdan, ya'ni parolli autentifikasiyalash protokoli asosida ochiq ko'rinishda uzatilishi;

b) shifrlash yoki bir yo'nalishli xesh-funksiya yordamida himoyalangan holda tarmoqqa uzatiladi.

Ko'pmartalik parollarni himoyalanganligi. Parollarni saqlash va uzatishda maksimal himoyalanganlik nuqtai nazaridan bir yo'nalishli funksiyalardan foydalangan ma'qul. Shu maqsadda kriptografik bardoshli xesh funksiyalardan foydalaniladi. Bu holda serverda parolni obrazi (etaloni) saqlanadi. Tizimga parol kelib tushgandan keyin tizim bu parol uchun xesh-almashtirish bajaradi va hosil bo'lgan xesh qiymatni serverda saqlanayotgan etaloni bilan solishtiradi. Agar ular bir xil bo'lsa, parollar ustma-ust tushadi. Parolni server xotirasidagi etaloni buzg'unchini qo'lga tushib qolgan taqdirda ham u parolni o'zini hisoblab topishi amalda mumkin emas. Buni quyidagicha izohlash mumkin.

Parollar saqlanadigan ma'lumotlar bazasiga ega bo'lgan buzg'unchi P foydalanuvchining parolini bilolmaydi. O'zini P foydalanuvchi sifatida tizimga taqdim qilishi uchun buzg'unchi $h(x^*)=h(x)$ kolliziyani ta'minlovchi x^* ni aniqlashi lozim bo'ladi. Odatda parollarni xeshlashda kriptobardoshli bo'lgan xesh funksiyalardan foydalaniladi. Ammo, xesh qiymat fiksirlangan uzunlikka ega ekanligi e'tiborga olinsa, buzg'unchi yetarlicha katta vaqt oralig'ida katta hisoblash resurslari vositasida x parollarni saralash yo'li bilan $h(x)$ xesh qiymat kolliziyalar jadvalini tuzish imkoniga ega bo'lishligini payqash mumkin. Shuningdek, ko'p ishlatiladigan ayrim xesh funksiyalarning kolliziyalar jadvali internetda ham bo'lishi mumkin. Shu sababli kolliziyalar asosidagi hujumlarga qarshi turish uchun hozirgi kunda quyidagi usullar amaliyotda keng qo'llanilmoqda.

1. *Parollarni «tuzlash» usuli.* Xeshlashda parolga qo'shiladigan c bul vektori *tuz deyiladi*. Kompyuter tizimidagi parollar bazasida foydalanuvchi identifikatori, $h(c,x)$ va c saqlanadi. Buzg'unchi $h(x^*)=h(c,x)$ tenglikni bajaruvchi x^* kolliziyani topsa-da, ammo u x^* kolliziyadan parolni aniqlay olmaydi.

Misol sifatida mobil telefonlardagi SIM-kartalardan foydalanishni keltirish mumkin. Sub'ekt o'zining kartasi (autentifikasiyalash qurilmasi)ni telefonga joylashtiradi va telefon ulangan paytda PIN-kod (parol) ni kiritadi. Shuningdek, zamonaviy noutbuklarda panjallarni izlarini skanerlangan nusxasi kiritilgan. Tizimga kirish uchun sub'ekt biometrik tekshiruvdan o'tishi va undan so'ngina parolni kiritishi lozim bo'ladi.

Autentifikasiyalash jarayoni bir tomonlama (masalan, foydalanuvchi o'zining haqiqiylikini serverga isbotlashi) va ikkitomonlama yoki o'zaro (axborot almashinuvchilarning har biri boshqasini autentifikasiyalashi) bo'lishi mumkin. WINDOWS NT tizimiga kirish prosedurasi bir tomonlama, WINDOWS 2000 tizimida KERBEROS protokolidan foydalanish ikkitomonlama autentifikasiyalashga misol bo'ladi.

§3.2. Autentifikasiyalash usullari

Ko'pmartalik parollar bo'yicha autentifikasiyalash. Ma'lumki, kompyuter tizimida autentifikasiyalash usullaridan biri foydalanuvchi tomonidan kiritiladigan «login» (foydalanuvchining qayd qilingan ismi) va parol (faqatgina foydalanuvchiga ma'lum bo'lgan qandaydir maxfiy axborot) ni kiritishdan iborat. Bularning har ikkalasi birgalikda foydalanuvchining identifikatorini tashkil qiladi. Foydalanuvchining haqiqiy login-parol juftligi maxsus ma'lumotlar bazasida saqlanadi.

Oddiy autentifikasiyalash quyidagi umumiy algoritmgga ega:

1. Sub'ekt tizimga kirishi uchun ruxsat so'rash maqsadida o'zining shaxsiy identifikatorini kiritadi.
2. Kiritilgan ma'lumotlar autentifikasiyalash serveriga kelib tushadi, bu yerda u maxsus ma'lumotlar bazasida saqlanayotgan shaxsiy identifikator bilan solishtiriladi.
3. Maxsus ma'lumotlar bazasida saqlanayotgan shaxsiy identifikator bilan kiritilgan ma'lumotlar bir xil bo'lsa, autentifikasiyalash muvaffaqiyatli o'tkaziladi va sub'ektga kompyuter tizimiga kirishga ruxsat beriladi. Aks holda sub'ekt yana birinchi qadamdagi harakatni qaytadan boshlashi lozim bo'ladi.

generasiya qilingan parol birtomonlama funksiyadan ketma-ket foydalanish yoki tizim tomonidan beriladigan har bir yangi so'rovnomma vaqtida tizimga uzatilishi mumkin.

Ikkinchi usulda vaqtinchalik nishonlardan foydalaniladi. Bu texnologiyaga misol sifatida SecurIDni keltirish mumkin. Unda autentifikasiyalash ma'lum bir vaqt oraliqlarida tasodifiy sonlarni generasiya qilishga asoslangan. Maxfiy kalit faqatgina tizim bazasida va sub'ektning apparat qurilmasida saqlanadi. Sub'ekt tizimga kirish uchun ruxsat so'ragan vaqtda undan PIN-kodni va ushbu vaqtda apparat qurilmasida ko'rinib turgan, tasodifiy generasiya qilingan sonni ko'rsatish talab qilinadi. Tizim kiritilgan PIN-kodni va sub'ektning bazadagi maxfiy kalitini taqqoslab, tizim bazasidagi maxfiy kalit va joriy vaqt asosida tasodifiy sonni generasiya qiladi. Undan keyin generasiya qilingan son va sub'ekt tomonidan kiritilgan sonni bir xilligi tizim tomonidan tekshiriladi.

Uchunchi usul sub'ekt va tizim uchun yagona parollar bazasiga va ular o'rtasidagi yuqori aniqlikdagi sinxronizasiyalashga asoslangan. Har bir parol faqatgina bir martagina ishlatilishi mumkin. Shu sababli buzg'unchi sub'ekt tomonidan foydalanilgan parolga ega bo'lgan vaqtda parol yaroqsiz bo'lib qoladi.

Ko'p martalik parollardan foydalanishga nisbatan bir martalik parollar yuqori himoya darajasiga ega.

§3.3. Autentifikasiyalash protokollari turlari

Autentifikasiyalash prosedurasi kompyuterlar o'rtasida axborot almashinuvida foydalaniladi. Bunda aloqa kanallari himoyasini ta'minlovchi murakkab kriptografik protokollar ishlatiladi. Autentifikasiyalash aloqada ishtirok etuvchi har ikki ob'ekt uchun ham zarur bo'lganligi bois, autentifikasiyalash o'zaro bo'lishi lozim.

Eng sodda autentifikasiyalash protokoli – *bu parol bo'yicha ruxsat olish (Password Authentication Protocol, PAP)*. Uning mohiyati shundaki, sub'ekt haqidagi butun axborot (identifikator va parol) tarmoqda ochiq holda uzatiladi. Bu esa PAPning asosiy kamchiligidir, ya'ni buzg'unchi

2. *Bir martalik parollardan foydalanish usuli.* Har bir foydalanuvchi o'zining parollar ro'yxatini tuzadi. Ushbu parollarning har biri bir marta ishlatilganidan so'ng yo'qotiladi.

Ko'pmartalik parollardan foydalanishda ham bir qator kamchiliklar mavjud. Birinchidan, etalonli parol yoki uning xeshlashtirilgan obrazi autentifikasiyalash serverida saqlanadi. Ko'p hollarda parolni saqlash kriptografik almashtirishlarsiz, tizimli fayllarda saqlanadi. Unga kirish yo'lini topgan buzg'unchilar maxfiy axborotlarga ega bo'lishlari mumkin.

Ikkinchidan, sub'ekt ko'pmartalik parolni yodda saqlab (yozib) yurishga majbur bo'ladi. Bunday holatda buzg'unchi parolga osongina ega bo'lishi mumkin. Bundan tashqari sub'ektni o'zi parolni tanlaydigan bo'lsa, tizimning himoyalanganligi sezilarli darajada zaiflashadi. Ko'p hollarda parolni tuzishda lug'atlardagi ayrim so'zlardan yoki ularni kombinasiyalaridan foydalanishlari mumkin. Buzg'unchida vaqt yetarlicha bo'lsa, u oddiy saralash usulidan foydalanib, parolni aniqlashi mumkin. Tasodifiy parollardan yoki sub'ekt tanlagan parolini ishlatish muddatini qisqaroq bo'lishi, ya'ni vaqt o'tishi bilan parollarni o'zgartirib turishdan foydalanish bunday muammolardan qutulish chorasini yaratadi.

Bir martalik parol bo'yicha autentifikasiyalash. Buzg'unchi sub'ektning ko'pmartalik paroliga bir martagina ega bo'lib qolsa, u doimo maxfiy axborot olish imkoniyatiga ega bo'lib qoladi. Bu kamchilikdan *bir martalik parol (OTP – One Time Password)* ni qo'llash bilan qutulish mumkin. Bu usulni mohiyati shundan iboratki, parol tizimga bir martagina kirish uchun yaroqli, keyingi safar tizimga kirish uchun yangi parol talab etiladi. Bir martalik parol bo'yicha autentifikasiyalash mexanizmi qurilma va dasturlar bo'yicha ham realizasiya qilinishi mumkin.

Bir martalik paroldan foydalanish texnologiyasini quyidagilarga bo'lish mumkin:

- Sub'ekt va tizim uchun umumiy bo'lgan psevdotasodifiy sonlar generatoridan foydalanish;

- Yagona vaqt tizimi asosidagi vaqt nishonlaridan foydalanish;

- Sub'ekt va tizim uchun umumiy bo'lgan tasodifiy parollar bazasidan foydalanish.

Birinchi usulda sub'ekt va tizim uchun bir xil qiymatga ega bo'lgan psevdotasodifiy sonlar generatoridan foydalaniladi. Sub'ekt tomonidan

– tizim qabul qilingan xabarni oldingi maxfiy kalit yordamida dastlabki matnga o'giradi. Natijalar tartib nomeri 2 bo'lgan tasodifiy son bilan bir xil bo'lsa, o'zaro autentifikasiyalash muvaffaqiyatli o'tadi.

Yuqorida keltirilgan algoritm ko'p hollarda «qo'l siqish» deyiladi. Ikkala holda ham sub'ekt tizim bilan bir xil maxfiy kalitga ega bo'lgan hollarda autentifikasiyalash muvaffaqiyatli o'tadi.

Autentifikasiyalash protokollarini xavfsizligini ta'minlanish darajasiga yoki ma'lum bir turdagi hujumlarga qarshi turish imkoniyatlari bo'yicha ham klassifikasiyalash mumkin. Ushbu yondoshuvga asosan autentifikasiyalash protokollari quyidagi turlarga bo'linadi:

- oddiy autentifikasiyalash (parollardan foydalanishga asoslangan);
- qat'iy autentifikasiyalash (kriptografik usul va vositalardan foydalanishga asoslangan);
- isboti nol oshkoralikka asoslangan autentifikasiyalash.

Oddiy autentifikasiyalashni tashkillashtirish sxemasi parollarni saqlash usullari bilan ham farqlanadi:

1. Parollar o'qish va yozishdan himoyalash atributlari qo'yilgan holda, tizimli fayllarda ochiq holda saqlanadi. Bunda kriptografik mexanizmlar (shifrlash, bir tomonlama funksiyalar) dan foydalanilmaydi. Kamchiligi: agar buzg'unchi qanaqadir yo'llar bilan tizimda administrator huquqiga ega bo'lsa, unda tizimli fayllar va parollarga ega bo'lish imkoni mavjud bo'ladi. Parollarni ushbu tarzda saqlashni himoyasini kuchaytirish uchun parollar saqlanadigan fayllarni tashqi tashuvchilarda saqlash tavsiya etiladi.

2. Parollarni shifrlangan yoki xesh qiymati ko'rinishida saqlash ularni xavfsizroq saqlanishini ta'minlaydi. Kiritilgan parolni tekshirishda tizim ushbu parolni xesh qiymatini hisoblab, bu qiymatni parollar jadvalidagi foydalanuvchining loginiga mos keluvchi xesh obrazi bilan solishtiradi.

Autentifikasiyalash protokollari xarakteristikalarini. Ushbu xarakteristikalar quyidagilardan iborat:

➤ hisoblash samaradorligi – protokolni bajarish uchun zarur bo'ladigan amallar soni;

➤ kommunikasion samaradorlik, ya'ni autentifikasiyalashni amalga oshirish uchun zarur bo'ladigan xabarlar soni va ularning uzunliklari bilan xarakterlanuvchi ko'rsatkich;

osongina shifrlanmagan ma'lumotga ega bo'lish imkoniga ega bo'lishi mumkin.

Nisbatan murakkabroq bo'lgan autentifikasiyalash protokollari «savol-javob» prinsipiga asoslangan. Masalan, CHAP (Challenge-Handshake Authentication Protocol) protokoli.

«Savol-javob» protokoli prosedurasi kamida to'rtta bosqichdan iborat bo'lishi mumkin:

– sub'ekt o'zining shaxsiy identifikatoriga doir so'rovni tizimga jo'natadi;

– tizim tasodifiy sonni generasiya qiladi va uni sub'ektga jo'natadi;

– sub'ekt tizim tomonidan jo'natilgan sonni o'zining maxfiy kaliti yordamida shifrlaydi va uni tizimga jo'natadi;

– tizim olingan xabarni maxfiy kalit (sub'ekt ishlatgan kalit) yordamida tiklaydi (dastlabki matnga o'giradi). Tasodifiy son bilan natijalar bir xil bo'lsa, autentifikasiyalash muvaffaqiyatli o'tadi.

Shifrlashda va dastlabki matnga o'g'irishda qo'llaniladigan maxfiy kalit tarmoq bo'yicha uzatilmaydi, shu sababli buzg'unchi unga ega bo'la olmaydi. Ammo, sub'ekt smart-karta, mobil telefon kabi shifrlash qurilmalariga ega bo'lishi lozim.

O'zaro autentifikasiyalash protokollari prinsipi «savol-javob» protokollaridan uncha ko'p farq qilmaydi. Uni amalga oshirish prinsipi quyidagicha:

– sub'ekt o'zining shaxsiy identifikatori va tartib nomeri 1 bo'lgan, tanlab olingan tasodifiy sondan iborat bo'lgan so'rovnomanini tizimga jo'natadi;

– tizim qabul qilingan, tartib nomeri 1 bo'lgan tasodifiy sonni maxfiy kalit yordamida shifrlaydi va tartib nomeri 2 bo'lgan tasodifiy sonni generasiya qiladi hamda har ikkalasini sub'ektga jo'natadi;

– sub'ekt olingan sonni maxfiy kalit yordamida dastlabki matnga o'giradi va natijani tartib nomeri 1 bo'lgan tasodifiy son bilan taqqoslaydi. Natijalarning bir xilligi tizim sub'ekt foydalangan maxfiy kalitga ega ekanligini anglatadi;

– sub'ekt qabul qilingan, tartib nomeri 2 bo'lgan tasodifiy sonni maxfiy kalit yordamida shifrlaydi va natijani tizimga jo'natadi;

5. Buzg'unchi tomonidan parolni interaktiv tanlanishini oldini olish uchun parolni kiritishga bo'lgan urinishlar sonini cheklab qo'yish.

6. Buzg'unchi tomonidan parolni interaktiv tanlanishini oldini olish uchun parol noto'g'ri kiritilganda (on-line rejimda) parolni qayta kiritishga bo'lgan ruxsatni kechiktirish.

7. Parolni amal qilishini maksimal muddatini cheklovchi talablar samaradorligini ta'minlash maqsadida foydalanuvchi parolini majburiy almashtirish rejimidan foydalanish.

Parollarni to'liq saralash. Parollarni to'liq saralash parolda bo'lishi mumkin bo'lgan belgilar birikmalarini to'g'ridan-to'g'ri saralashdan iborat. Paroldagi belgilar soni va ularning turi (harflar, raqamlar, maxsus belgilar) ni belgilab, qidiruvni bir muncha qisqartirish mumkin. Quyida keltirilgan 4.1-jadvalda parollarni to'liq saralashga sarf bo'ladigan vaqtni parollar uzunligiga bog'liqligi <http://www.password-crackers.ru/articles/12#> internet manzili asosida keltirilgan (bunda parollarni saralash tezligi 10^6 parol/sekunddan iborat).

Alifbo	Alifbo belgilar soni	3 ta belgili parolni buzish vaqti	6 ta belgili parolni buzish vaqti	8 ta belgili parolni buzish vaqti	12 ta belgili parolni buzish vaqti
Kichik lotin harflari	26	0,02 sek	5 min	58 soat	3000 yil
Kichik lotin harflari va raqamlar	36	0,04 sek	36 min	32 kun	150 000 yil
Kichik va katta lotin harflari hamda raqamlar	62	0,02 sek	15 soat	7 yil	100 mln yil
Kichik va katta lotin harflari hamda raqamlar va maxsus belgilar	95	1 sek	8 kun	193 yil	Er mavjud bo'lgandan ham ko'proq vaqt talab qilinadi

➤ uchinchi ishtirokchining mavjudligi, masalan, simmetrik kalitlarni taqsimlashni tashkillashtiruvchi ishonchli server uchinchi ishtirokchi sifatida ishtirok etishi mumkin;

➤ xavfsizlik kafolatining asoslari, masalan, oshkoraligi nol bo'lgan protokollar;

➤ maxfiylikni saqlash usullari, ya'ni kalitli axborotlarni saqlash usullari.

§3.4. Parol bo'yicha autentifikasiyalashga hujumlar va ularni bartaraf qilish

Parol bo'yicha autentifikasiyalashga asosiy tahdid – bu parolni buzish, ya'ni tizimga kirish huquqini beruvchi foydalanuvchi parolini buzg'unchi tomonidan ochilishidir. Bu yerda asosiy hujum turlari quyidagilardan iborat:

1. Parollarni to'liq saralash.

2. Lug'at yordamida hujum tashkil qilish.

3. Kamalakli jadval yordamida hujum tashkil qilish.

4. Ijtimoiy injeneriya usuli (mazkur usul foydalanuvchi parol sifatida o'zining shaxsiy ma'lumotlari – ismi, familiyasi, tug'ilgan yili kabi ma'lumotlardan foydalanishga asoslangan).

5. Parolni tutish uchun zararkunanda dasturlarni o'rnatish.

6. Tarmoq ishonchli ob'ektini o'zgartirish (IP-spoofing).

7. Paketlarni tutib qolish (sniffing).

Inson faktori ta'sirini kamaytirish uchun parollarni tanlash va ulardan foydalanishda quyidagilarga amal qilish maqsadga muvofiq:

1. Parollarni to'liq saralashni qiyinlashtirish maqsadida parollarni minimal uzunligini belgilash.

2. Parollarni saralashni murakkablashtirish uchun parollarni nomlashda turli guruhlardagi belgilardan foydalanish.

3. Buzg'unchi tomonidan lug'at yordamida hujum tashkil qilishni qiyinlashtirish maqsadida lug'at bo'yicha parollarni tekshirish va ularni bekor qilish.

4. Parollarni to'liq saralash usulini murakkablashtirish uchun parollardan foydalanishning maksimal muddatini belgilash.

Lug'at yordamida hujum tashkil qilishda muvaffaqiyat ehtimoli lug'at yordamidagi hujum natijasida topilgan parollar sonining urinishlarning umumiy soniga bo'lgan nisbatiga teng.

Parollarni to'liq yoki lug'at yordamida saralashda PasswordsPro, MD5BFCPF, John the Ripper dasturlaridan foydalanish mumkin.

Lug'at yordamida online hujumga qarshi kurashish. Ushbu turdagi hujumga qarshi kurashish uchun quyidagilardan foydalanish tavsiya qilinadi:

1. Javobni kechiktirish (delayed response): taqdim qilingan login/parol juftligiga server uncha katta bo'lmagan, maxsus generatsiya qilingan kechikish bilan javob berishdan foydalanadi (masalan, sekundga bittadan ortiq bo'lmagan javob bilan).

2. Login/parol juftligini bir necha marta, ketma-ket xato taqdim qilingan hollarda qayd qilish yozuvini blokirovka qilish (account locking) (masalan, parolni kiritish bo'yicha ketma-ket 5 marta muvaffaqiyatsiz harakatlardan so'ng bir soatga blokirovka qilish).

Bu ikki usul lug'at yordamida saralashni amalga oshirishga va nisbatan kichik vaqt oralig'ida parolni buzishga xalaqit beradi.

3. Login/parol juftligini to'g'ri kiritish fizik shaxs tomonidan, lug'at yordamida saralash esa kompyuter vositasida maxsus dastur asosida amalga oshiriladi deb faraz qilinadi. Shu bois, parolni to'g'ri kiritish inson uchun hisoblash nuqtai nazaridan oddiy, kompyuter dasturi uchun murakkab bo'lishi lozim. Server insonni kompyuter dasturidan farq qilishi uchun CAPTCHA dan foydalanadi (masalan, login/parol juftligini kiritishdan oldin qandaydir tasvirdan foydalanuvchi testdan foydalanadi).

Lug'at yordamida offline hujumga qarshi kurashish. Parolni xeshlashda parolga tasodifiy bitlar ketma-ketligi (bu tasodifiy bitlar ketma-ketligi tuz nomlanadi) qo'shiladi. Natijada parolning uzunligi ortadi. Bu esa o'z navbatida lug'at yordamida offline va kamalakli jadval yordamidagi hujumlarni amalga oshirishga to'sinlik qiladi.

Parol mustahkamligini miqdoriy baholash. Faraz qilaylik, parol alifbosi quvvati A bilan, uning uzunligi L bilan belgilansin. U holda $S = A^L$ - uzunligi L bo'lgan parollar sonini ifodalaydi. Shuningdek, v - buzg'unchi tomonidan parollarni saralash tezligi, T - parolni amal

Jadvalni izohlashni hojati yo'q. AQSHning standartlar va texnologiyalar milliy instituti (NIST) parollarni eng yaxshi himoyasi sifatida ularni 95 belgili alifbo (ASCII nabori) dan foydalanib, 12 ta belgi shaklida ifodalashni tavsiya qiladi.

Kuchsiz parollarni generatsiya qilishga sabab bo'luvchi faktorlar (xatolar). Quyida keltirilgan parollar oddiy shablonga asoslangan. Shu sababli ularni tez topish mumkin.

➤ O'z vaqtida kompyuter so'roviga javob bermaslik sababli kompyuter o'zi tanlaydigan parollar: default, admin, guest va boshqalar.

➤ Lug'atdagi so'zlar: chameleon, RedSox, sandbags, bunnyhop! va ingliz tili lug'atida mavjud bo'lmagan belgilar birikmalari.

➤ So'zlar va sonlar birikmalari: password1, deer2000, ivan1234, petrov1980. Bu birikmalarni oson topish mumkin.

➤ Harflari boshqa belgilar bilan almashtirilgan so'zlar: p@ssword, 133th4xor, g0ldf1sh.

➤ Ikkilangan so'zlar: crabcrab, stopstop, treetree, passpass, ivanivan.

➤ Klaviaturada ketma-ket yoki bir-biriga yaqin joylashgan belgilar ketma-ketligi: qwerty, 12345, asdfgh, fred, aszx.

➤ Yaxshi ma'lum bo'lgan naborlarga asoslangan sonlar ketma-ketligi: 12345, 911, 271828, 314159.

➤ Foydalanuvchining shaxsiy ma'lumotlari: telefon nomeri, STIR. PIN-kodi va boshqalar.

Lug'at yordamida hujum tashkil qilish. Lug'at yordamida hujum tashkil qilish (dictionary attack) – parollarni to'liq saralashga asoslangan, himoya tizimiga qilinadigan hujum turiga mansub. Unda ma'lum bir turga va uzunlikka ega bo'lgan lug'atdagi so'zlar hujum qilish uchun tanlanadi. Lug'atlar namunalari <http://passwords.ru> internet manzilida keltirilgan. Hujum parol sifatida qandaydir tilga mansub bo'lgan so'z yoki ibora foydalanilgan degan farazga asoslangan. Bunday hujumlarning 2 turi mavjud:

1. *Online hujum.* Bunda parolni to'g'riligini tekshirish uchun server doimiy muloqatda bo'lishi lozim.

2. *Offline hujum.* Bunda parolni to'g'riligini tekshirishni server bilan aloqa o'rnatmasdan hujumchining o'zi parolni saralashni (masalan, kamalakli jadval usulidan foydalanib) amalga oshiradi.

4. Solishtirish natijasi ijobiy bo'lsa, foydalanuvchi autentifikasiyalash jarayonidan muvaffaqiyatli o'tadi, tizim esa foydalanuvchi autentifikasiyalash seanslari sonini hisoblab boruvchi hisoblagichni qiymatini bittaga oshiradi, ya'ni endi $i = i+1$ bo'ladi.

Lampport protokolining asosiy kamchiligi shundan iboratki, unga nisbatan buzg'unchi «o'rtada odam» turidagi hujumni uyushtirishi mumkin. Ushbu protokolda tizim foydalanuvchi tomonidan autentifikasiya qilinmasligi bois, tizim o'rniga buzg'unchi tizim nomidan foydalanuvchi bilan aloqa o'rnatishi mumkin. Masalan, navbatdagi i -chi seansda tizim foydalanuvchiga i sonini jo'natmasdan oldinroq tizim nomidan buzg'unchi foydalanuvchiga hisoblagichning joriy i qiymatiga nisbatan katta bo'lgan j sonini jo'natishi mumkin. Natijada buzg'unchi foydalanuvchidan $H^{N^j}(W)$ qiymatni qabul qilishi mumkin. Ushbu qiymat asosida buzg'unchi

$$H^{N^j}(W), \dots, H^{N^i}(W)$$

diapazondagi ixtiyoriy qiymatni hisoblash imkoniyatiga ega bo'ladi. Ushbu hujumni oldini olish uchun parol faqatgina autentifikasiyadan o'tgan tomonga berilishi lozim. Shu sababli bunday turdagi xavflarni bartaraf etish uchun «savol-javob» turidagi autentifikasiyalash protokollaridan foydalanish tavsiya etiladi.

§3.6. «Savol-javob» turidagi autentifikasiyalash protokollari

«Savol-javob» turidagi autentifikasiyalash protokollarining mohiyati shundan iboratki, autentifikasiyalashdan o'tish uchun bir ishtirokchi (foydalanuvchi) ikkinchi ishtirokchi (tizim) ga qandaydir maxfiy axborot (sir) ni bilishini namoyish qilish orqali o'zining autentligini isbotlashi lozim bo'ladi. Bunda o'zining autentligini isbotlovchi ishtirokchi vaqt bo'yicha o'zgarib boruvchi savollarga javob berishi kerak bo'ladi. Javob esa uning siriga va beriladigan savolga bog'liq bo'ladi. Odatda savol sifatida protokolni boshida tanlab olingan son ishtirok etadi.

Ushbu protokolda seansni takrorlash asosidagi hujumni oldini olish uchun vaqt bo'yicha o'zgarib boruvchi parametrlardan foydalaniladi.

Autentifikasiyalash protokollarining xalqaro standarti.

qilishning maksimal muddati bo'lsin. T vaqtda parolni saralash ehtimolini quyidagicha aniqlash mumkin:

$$P = \frac{\nu T}{S} = \frac{\nu T}{A^L}.$$

Barcha parollar sonining quyi chegarasi quyidagicha bo'ladi:

$$S^* = \left\lceil \frac{\nu T}{P} \right\rceil.$$

§3.5. Foydalanuvchini autentifikasiya qilishning Lamport protokoli

Tayyorgarlik bosqichi:

1. Foydalanuvchi va tizim ular o'rtasidagi bo'lishi mumkin bo'lgan bog'lanishlar soni N (bu son maxfiy saqlanadi) haqida kelishib oladilar.

2. Foydalanuvchi W (uzunligi 128 bit va undan ortiq) parolni tanlaydi va ushbu parolni ketma-ket N marta xeshlaydi. Hosil bo'lgan

$$H(W) = H^1(W),$$

$$H(H(W)) = H^2(W),$$

$$H(H(H(W))) = H^3(W),$$

.....

$$H(H(H(\dots H(W)))) = H^N(W)$$

xesh qiymatlar ketma-kelgini himoyalangan kanal orqali maxfiy tarzda tizimga uzatadi.

3. Tizim foydalanuvchini autentifikasiyalash seanslari sonini hisoblab borish uchun hisoblagichga 1 sonini yozadi.

Autentifikasiyalashning i -chi seansi.

1. Tizim foydalanuvchiga i sonini jo'natadi.

2. Foydalanuvchi W parolni $N-i$ marta xeshlaydi va hosil bo'lgan natija $H^{N-i}(W)$ tizimga jo'natadi.

3. Tizim $H(H^{N-i}(W)) = H^{N-i+1}(W)$ ni hisoblaydi va natijani o'zida saqlanayotgan $H^{N-i+1}(W)$ ni qiymati bilan solishtiradi.

kirishga ruxsat oladi. Agar foydalanuvchida ham serverda ham taymer bo'lsa, foydalanuvchi birdaniga vaqt nishoni qo'shilgan xabarni serverga jo'natishi mumkin. Server esa bu vaqt nishonini o'zidagi vaqt bilan solishtirib ko'rishi mumkin bo'ladi.

Tasodifiy sonlardan foydalanib, bir tomonlama autentifikasiyalash.

1. $P \rightarrow S: \text{login/parol};$
2. $P \leftarrow S: r;$
3. $P \rightarrow S: E_k(r);$
4. $S: r^* = D_k(E_k(r)).$

P foydalanuvchi server S ga o'zining login/parol justligini jo'natgandan so'ng, server savol sifatida psevdotasodifiy sonlarni ishlab chiquvchi generator orqali hosil qilingan r tasodifiy sonni foydalanuvchiga jo'natadi. Bu sonni qabul qilgan foydalanuvchi uni umumiy bo'lgan k kalit bilan shifrlab, server S ga jo'natadi. Server o'z navbatida shifrlangan ma'lumotni dastlabki matnga o'girib, $r^* = r$ ni tekshirib ko'radi. Agar ushbu qiymatlar teng bo'lsa, u holda foydalanuvchi autentifikasiyalashdan muvaffaqiyatli o'tadi.

Tasodifiy sonlardan foydalanib, o'zaro autentifikasiyalash.

1. $P \rightarrow S: \text{login/parol};$
2. $P \leftarrow S: r_1;$
3. $P \rightarrow S: E_k(r_1, r_2);$
4. $P \leftarrow S: D_k(E_k(r_1, r_2)), E_k(r_2, r_1);$
5. $P: D_k(E_k(r_2, r_1)).$

Ortiqcha izohlashning hojati yo'q. Bu yerda r_1, r_2 – mos holda server va foydalanuvchi tomonidan generatsiya qilingan tasodifiy sonlar. Protokolning 3-chi qadamida P foydalanuvchi server S tomonidan autentifikasiyalanmoqda. Xuddi shuningdek, 5-qadamda S server P foydalanuvchi tomonidan autentifikasiyalash jarayonidan o'tmoqda. Ya'ni, bu protokolda ishtirokchilar navbat bilan isbotlovchi va tekshiruvchi vazifalarini bajarishmoqda. ISO/IEC 9798-4 standartida ko'rsatilganidek ushbu protokolda E_k shifrlash funksiyasini o'rniga kalitli xesh funksiyadan

Standartlashtirish bo'yicha xalqaro tashkilot va xalqaro elektrotexnika komissiyasining ISO/IEC 9798 - Information technology - Security techniques - Entity authentication mechanisms standarti autentifikatsiyalash protokollarining asosiy xalqaro standarti hisoblanadi. Ushbu standart quyidagi 5 ta qismdan iborat:

1. ISO/IEC 9798-1 – «General Model»;
2. ISO/IEC 9798-2 – «Mechanisms using symmetric encipherment algorithms»;
3. ISO / IEC 9798-3 – «Entity authentication using a public-key algorithm»;
4. ISO / IEC 9798-4 – «Mechanisms using a cryptographic check function»;
5. ISO / IEC 9798-5 – «Mechanisms using zero knowledge techniques».

Ushbu standart bo'yicha tavsiya qilingan ayrim protokollar quyida keltiriladi.

§3.7. Simmetrik kriptosxemalardan foydalanuvchi «savol-javob» protokollari

Ushbu protokollarda autentifikatsiyalashdan o'tuvchi va tekshiruvchi tomon simmetrik kalitlarga ega deb faraz qilinadi. Ushbu kalitlarga ega bo'lish uchun real vaqt rejimida ishlovchi ishonchli markaz xizmatidan foydalanish mumkin. ISO/IEC 9798-2 («Mechanisms using symmetric encipherment algorithms») standartida autentifikatsiyalashning quyidagi 3 ta usuli keltirilgan.

Vaqt nishoniga asoslangan bir tomonlama autentifikatsiyalash.

1. $P \rightarrow S: E_k(t_p)$;

2. $S: t_p^* = D_k(E_k(t_p))$.

P foydalanuvchi t_p vaqtni umumiy bo'lgan k kalit bilan shifrlab, server S ga jo'natadi. Server o'z navbatida shifrlangan ma'lumotni dastlabki matnga o'girib, $t_p^* = t_p$ ni hosil qiladi. Agar ushbu qiymat serverda taymer vaqtiga yaqin bo'lsa, u holda foydalanuvchi tizimga

nazarda tutadi. Bu dasturlash tizimi quyidagi 2 ta asosiy qismdan tashkil topgan:

- *Kerberosning mijoz qismi*. Kerberos serveri komponentalari o'rnatilmagan himoyalangan tarmoqning barcha kompyuterlarida mijoz qismi o'rnatiladi. Protokol bo'yicha xabar almashinuvida xizmat qiluvchi dasturiy ta'minot o'rnatilgan va qandaydir foydalanuvchi qayd qilingan kompyuter Kerberos mijoz bo'ladi. Ayrim hollarda tarmoq serverlari (faylli serverlar, bosma serverlari va boshqalar) ham mijoz sifatida ishtirok etishi mumkin;

- *Kerberosning server qismi*. Bu qism Kalitlarni tarqatish markazi (inglizcha KDS - «Key Distribution Center») deb nomlanadi hamda uning o'zi autentifikasiyalash serveri (inglizcha AS - «Authentication Server») va ruxsatnoma berish serveri (inglizcha TGS - «Ticket Granting Server») deb nomlanuvchi tashkil etuvchilardan iborat.

Shunday qilib, Kerberos sxemasi 3 ta dasturiy komponentalar - mijoz C, Kerberos serveri va SS (inglizcha «Service Server» so'zidan olingan) serverlarning o'zaro axborot almashinuidan iborat. Bu yerda SS tarmoq mijozlariga xizmatlar ko'rsatuvchi serverdir. Ayrim hollarda SS server boshqa serverning mijoz bo'lishi ham mumkin (masalan, bosma serveri fayllar serveri xizmatidan foydalaninshi mumkin).

Mijoz C tarmoq serveri SS xizmatidan foydalanish uchun AS autentifikatordan ruxsat olishi lozim. Ruxsatnoma TGS serveri bilan aloqa o'rnatish huquqini beruvchi bilet korinishida bo'lib, u autentifikasiyalash serveri AS tomonidan beriladi. Bu bilet TGS - ruxsatnoma berish serveriga mijoz tomonidan taqdim qilinadigan, shifrlangan ko'rinishdagi ma'lumotdir. Birinchi ruxsatnomadan boshqa barcha ruxsatnomalarni mijoz TGS serveridan oladi. TGS serverining o'ziga murojaat qilishga ruxsat beruvchi birinchi ruxsatnomani mijozga autentifikasiyalash serveri AS beradi (3.1-rasm)

foydalanish mumkin. Protokolni mustahkamligini oshirish maqsadida uzatilayotgan xabarga vaqt nishonini ham qo'shish mumkin.

O'zaro autentifikasiyalash har bir ishtirokchiga ma'lum bo'lgan umumiy sir asosida (bunday yondoshuv «o'zimizniki-begona» tizimlarida qo'llaniladi), Shuningdek, ishtirokchilar umumiy sirga ega bo'lmagan hollarda, ishtirokchilarning ochiq kalitlari saqlanadigan biron bir ishonchli markaz orqali amalga oshiriladi. «O'zimizniki-begona» tizimlaridan foydalanuvchi protokollar «qo'l siqishish» protokollari deb nomlanadi.

§3.8. Kerberos protokoli

Kerberos protokoli XX asming 80-yillari o'rtalarida Nidxem-Shrederning uchinchi ishonchli tomon ishtirokidagi autentifikasiyalash va simmetrik shifrlash kalitlarini tarqatish protokoli negizida yaratilgan. Protokolda uchinchi ishonchli tomon sifatida Kalitlarni tarqatish markazi ishtirok etadi.

Ushbu protokol ommaviylashgan operasion tizimlar - Unix, Windows (Windows 2000 dan boshlab) operasion tizimlari oilalarida, shuningdek, Mac OS da asosiy autentifikasiyalash protokoli sifatida realizasiya qilingan. Bu protokol ochiq tizimlarda ham, shuningdek, SSH da ham qo'llanilgan. Protokolda sfifrlash jarayoni DES sfifrlash algoritmi asosida amalga oshiriladi va albatta, ushbu maqsadda boshqa algoritmlar ham qo'llaninishi mumkin.

Kerberos protokoli «mijoz-server» arxitekturasi asosida yaratilgan bo'lib, simmetrik shifrlash kalitlarini tarqatish va himoyalanmagan tarmoqdagi foydalanuvchilarni haqiqiyiligini markazlashgan tizim asosida tekshirishga mo'ljallangan. Bunda himoyalanmagan aloqa kanalidagi ikkita ishtirokchi (xostlar) aloqa o'rnatishdan oldin o'zaro autentifikasiyalashdan o'tishadi. Hozirgi kunda Kerberos protokoli autentifikasiyalash serverining amaldagi standarti vazifasini bajarmoqda.

Kerberos protokolining bir necha variantlari mavjud bo'lib, ularning hammasi bitta g'oyaga asoslangan. Protokolni amalga oshirish «mijoz-server» arxitekturasi asosida qurilgan dasturlash tizimidan foydalanishni

K_{AS_TGS} – autentifikasiyalash va ruxsatnoma berish serverlari uchun umumiy bo'lgan, maxfiy kalit;

TGT (inglizcha «Ticket Granting Ticket») – ruxsatnoma berish serveri TGS bilan aloqa o'rnatish huquqini beruvchi bilet. Uning mazmuni $\{TGT\} = \{c, tgs, t_1, p_1, K_{C_TGS}\}$ dan iborat;

tgs – TGS serverining identifikatori;

t_1 – vaqt nishoni;

p_1 – biletning amal qilish muddati.

$\{...\}KX$ – figurali qavs ichidagi ma'lumot KX kalit bilan shifrlanganini anglatadi.

Bu qadamda autentifikasiyalash serveri AS mijoz o'zining ma'lumotlar bazasida qayd etilganligini tekshirib, ishonch hosil qilgandan so'ng, unga ruxsatnoma berish serveri TGS bilan aloqa o'rnatish huquqini beruvchi bilet va server bilan aloqada foydalanish uchun kalitni jo'natdi. Bu jo'natma mijozning maxfiy kaliti bilan shifrlangan. Biroq, jo'natmani qabul qilgan haqiqiy C mijoz biletini mazmuni bilan tanishish imkoniyatiga ega emas. Chunki bilet autentifikasiyalash va ruxsatnoma berish serverlari uchun umumiy bo'lgan, maxfiy K_{AS_TGS} kalit bilan shifrlangan. Shuni ham qayd etish lozimki, birinchi qadamda c identifikatori C mijoz emas, balki qandaydir buzg'unchi jo'natgan bo'lsa, AS serverdan olingan jo'natmani ushbu buzg'unchi ochiq matn ko'rinishiga o'gira olmaydi.

3. $C \rightarrow TGS : \{TGT\}K_{AS_TGS}, \{Aut_1\}K_{C_TGS}, \{ID\}$.

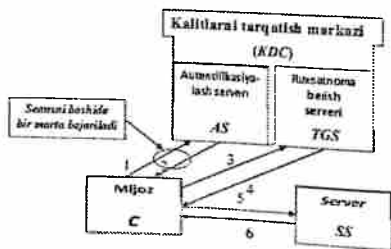
Bu yerda quyidagi belgilashlar ishlatilgan:

$\{Aut_1\}$ – mazmuni $\{Aut_1\} = \{c, t_2\}$ bo'lgan autentifikasiyalash bloki;

t_2 – vaqt nishoni;

ID – so'ralayotgan xizmat turining identifikatori (xususan, SS serverning identifikatori ham bo'lishi mumkin).

Ushbu qadamda mijoz AS serverdan qabul qilgan TGT biletini shifrlangan holda hamda mijoz identifikatori va jo'natma shakllantirilgan vaqtni anglatuvchi vaqt nishonidan iborat bo'lgan autentifikasiyalash bloki $\{Aut_1\}$ ni ruxsatnoma berish serveri TGS ga jo'natadi.



3.1-rasm. Kerberos protokolinig ishlash sxemasi.

Ruxsatnoma maxfiy kalit bilan shifrlangan ma'lumot bo'lib, bu kalit faqatgina Kerberos serverlari AS va TGSga ma'lum. Shu sababli ruxsatnomani birinchi qabul qiluvchi, masalan, mijoz bu ruxsatnoma aynan Kerberos serveridan berilganligiga shubhalanmasa ham bo'ladi.

Odatda ruxsatnomalar ma'lum bir vaqt oralig'ida, ya'ni ko'p martali foydalanishga mo'ljallangan bo'ladi. Bu muddat tugashi bilan mijoz yana qaytadan autentifikatsiyalashdan o'tishi lozim bo'ladi. Har safar aloqa o'rnatilganda vaqt nishonidan foydalaniladi. Shu sababli tarmoqda yagona vaqt xizmatidan foydalanish maqsadga muvofiq.

Faraz qilaylik, C mijoz tarmoq mijozlariga xizmatlar ko'rsatuvchi SS server xizmatidan foydalanishni istaydi. Bu holda Kerberos protokolidan foydalanish quyida keltirilgan qadamlar ketma-ketligini amalga oshirishdan iborat bo'ladi.

$$1. C \rightarrow AS : \{c\}.$$

Mijoz C autentifikatsiyalash serveri AS ga o'zining identifikatorini ochiq holda jo'natmoqda.

$$2. AS \rightarrow C : \{ \{ \{ TGT \} \}_{K_{AS_TGS}}, K_{C_TGS} \}_{K_C}.$$

Bu yerda quyidagi belgilashlardan foydalanilgan:

K_C – mijozning maxfiy simmetrik shifrlash kaliti;

K_{C_TGS} – ruxsatnoma berish serveri TGS bilan aloqa o'rnatish uchun

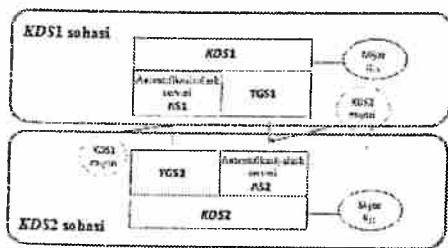
mijozga berilgan kalit;

$$6. SS \rightarrow C : \{t_4 + 1\}K_{C_SS}.$$

Ushbu qadamda *SS* server o'zini haqiqiyligini mijozga isbotlashi lozim. U bu ishni 5-qadamdagi xabarni ochiq matn ko'rinishiga to'g'ri o'girganligini ko'rsatish bilan bajarishi mumkin. Shu maqsadda u mijozning autentifikatsiyalash blokidan t_4 vaqt nishonini oldindan belgilangan qoida bo'yicha o'zgartiradi (unung qiymatini bir birlikga oshiradi). Hosil bo'lgan natijani mijoz bilan umumiy bo'lgan, maxfiy K_{C_SS} kalit bilan shifrlab, mijozga jo'natadi.

Agar bu yerda keltirilgan barcha qadamlar to'g'ri bajarilgan va barcha tekshiruvlar ijobiy yakunlangan bo'lsa, u holda *C* va *SS* ishtirokchilar bir-birlarining haqiqiyligiga ishonch hosil qildilar hamda himoyalangan aloqa seansi o'rnatish uchun K_{C_SS} maxfiy kalitga ega bo'ldilar.

Shuni ham ta'kidlash lozimki, aloqa seansi ish jarayonida *AS* autentifikator tomonidan faqat bir marta mijozning haqiqiyligi tekshiriladi, ya'ni protokolning 1-,2-qadamlari bir marta bajariladi. Agar mijoz boshqa server (masalan, *SS1*) xizmatidan foydalanishni xohlasa, u holda mijoz o'zidagi *TGT* bilet bilan ruxsatnoma berish *TGS* serveriga murajaat qiladi. Bu vaziyatda protokol 3-qadamdan boshlab amalga oshiriladi.



3.2-rasm. Kerberos sohalarining bir-biri bilan o'zaro ta'siri.

Kerberos protokolidan foydalanishda kompyuter tarmog'i mantiqan Kerberos serveri ta'siri ostidagi cohalarga bo'linadi (3.2-rasm).

Foydalanuvchi va serverlari qandaydir bitta Kerberos serveri ma'lumotlar bazasida qayd qilingan tarmoq qismi yoki hududi Kerberos

TGS ruxsatnoma berish serveri *TGT* biletni ochiq matn ko'rinishiga o'giradi va undan bilet kimga, qachon, qanday muddatga berilgani hamda *AS* server tomonidan mijoz bilan maxfiy aloqa o'rnatish uchun berilgan K_{C_TGS} kalit haqida axborotga ega bo'ladi. K_{C_TGS} kalitdan foydalanib, $\{Aut_1\}$ autentifikasiyalash blokini ochiq matn ko'rinishiga o'giradi. Autentifikasiyalash blokidagi vaqt nishoni biletdagi vaqt nishoni bilan ustma-ust tushsa, jo'natmani haqiqatan ham *C* mijoz jo'natganiga ishonch hosil qiladi. Chunki, faqat *C* mijoz K_{C_TGS} kalitni biladi va shu sababli faqat u o'zining identifikatorini to'g'ri shifrlashi mumkin. Undan so'ng biletni amal qilish muddati va 3-qadamdagi jo'natmani jo'natish vaqti tekshiriladi. Agar biletni amal qilish muddati tugamagan bo'lsa, u holda 4-qadam bajariladi.

$$4. TGS \rightarrow C : \{ \{TGS\}K_{TGS_SS}, K_{C_SS} \} K_{C_TGS}.$$

Bu yerda quyidagi belgilashlardan foydalanilgan:

K_{TGS_SS} – *TGS* va *SS* serverlarining umumiy maxfiy kaliti;

K_{C_SS} – mijoz va *SS* serverining umumiy maxfiy kaliti;

$\{TGS\}$ – *SS* serveri bilan aloqa o'rnatish huquqini beruvchi bilet. Uning mazmuni $\{TGS\} = \{c, ss, t_3, P_2, K_{C_SS}\}$ dan iborat;

ss – *SS* serverining identifikatori.

Ushbu qadamda *C* mijoz *SS* serveri bilan aloqa o'rnatish uchun K_{C_SS} shifrlash kaliti va $\{TGS\}$ biletni ruxsatnoma berish serveri jo'natmoqda. $\{TGS\}$ biletni mazmuni 2-qadamdagi $\{TGT\}$ biletni mazmuni bilan bir xil.

$$5. C \rightarrow SS : \{ \{TGS\}K_{TGS_SS}, \{Aut_2\}K_{C_SS} \}.$$

Bu yerda *C* mijoz *SS* serveri bilan himoyalangan aloqa o'rnatish uchun $\{TGS\}$ biletni shifrlangan holicha va $\{Aut_2\} = \{c, t_2\}$ autentifikasiyalash blokini *SS* serverga jo'natmoqda. *SS* server K_{TGS_SS} maxfiy kalitdan foydalanib, $\{TGS\}$ biletni ochiq matn ko'rinishiga keltiradi va bu matndagi K_{C_SS} kalitdan foydalanib, xabarni jo'natuvchisini haqiqiylikini tekshirib ko'radi.

muvaqqiyatli verifikasiyadan o'tsa, tizimga kirish uchun foydalanuvchi ruxsatga ega bo'ladi.

Elektron raqamli imzo va tasodifiy songa asoslangan bir tomonlama autentifikasiyalash.

1. $P \rightarrow S$ login/parol;
2. $P \leftarrow S: r_1$;
3. $P \rightarrow S: cert_A, r_1, V, S_A(r_1, r_2, V)$.

Bu yerda $cert_A - A$ foydalanuvchining ochiq kaliti sertifikat, r_1, r_2 - mos holda server va foydalanuvchi tomonidan generasiya qilingan tasodifiy sonlar, V - server identifikatori, S_A - foydalanuvchi imzosi. Imzo muvaqqiyatli verifikasiyadan o'tsa, tizimga kirish uchun foydalanuvchi ruxsatga ega bo'ladi.

Elektron raqamli imzodan foydalanib, o'zaro autentifikasiyalash.

1. $P \rightarrow S$ login/parol;
2. $P \leftarrow S: r_1$;
3. $P \rightarrow S: cert_A, r_1, V, S_A(r_2, r_1, V)$;
4. $P \leftarrow S: cert_V, P, S_V(r_1, r_2, P)$.

Bu yerda $cert_A$ - foydalanuvchining ochiq kaliti sertifikat, $cert_V$ - serverning ochiq kaliti sertifikat, r_1, r_2 - mos holda server va foydalanuvchi tomonidan generasiya qilingan tasodifiy sonlar, V - server identifikatori, S_A - foydalanuvchi imzosi. Imzo muvaqqiyatli P - foydalanuvchi identifikatori, tizimga kirish uchun foydalanuvchi ruxsatga ega bo'ladi.

§3.10. Ochiq shifrlash sxemalariga asoslangan o'zaro autentifikasiyalash protokoli

1. $P \rightarrow S: r_1, E_{K_C, otkr}(r_1, A)$;
2. $P \leftarrow S: r_2, E_{K_A, otkr}(r_1, r_2)$;
3. $P \rightarrow S: D_{K_A}(E_{K_A, otkr}(r_1, r_2)), r_2$.

sohasi deyiladi. Bitta Kerberos sohasi bir necha bir-biri bilan bog'langan lokal tarmoqlarni birlashtirishi mumkin.

Kerberos sohalari bir-birlari bilan aloqa qilishlari uchun Kerberos serverlari bir-birlarida o'zaro qayddan o'tgan bo'lishlari lozim. Buning natijasida bir sohaning ruxsat beruvchi serveri boshqa sohaning mijozlari sifatida qayd qilinadi va uning autentifikasiyalash serveri ma'lumotlar bazasiga kiritilib, bu sohaning xizmatlaridan foydalanish uchun tegishli maxfiy kalitga ega bo'ladi.

O'zaro kelishuvlar o'rnatilganidan, ya'ni bir-birlarida o'zaro qayddan o'tganlaridan so'ng Kerberosning ikki sohasi mijozlari bir-birlari bilan aloqa qilishlari mumkin. Masalan, 3.2-rasmdagi birinchi *KDS1* sohasining mijozlari K_{11} ikkinchi *KDS2* sohasining K_{21} mijozlari bilan aloqa seansini o'rnatishi mumkin. Buning uchun K_{11} mijoz *KDS2* sohasining Kerberos serveri bilan aloqa o'rnatish huquqini beruvchi biletni o'zining ruxsatnoma berish serveri TGS1 dan olishi lozim. Ushbu biletta biletning egasi qaysi Kerberos sohasida qayd qilinganligi haqida ma'lumot bo'ladi. Bilet *KDS1* va *KDS2* Kerberos sohalari uchun umumiy, maxfiy kalit bilan shifrlangan bo'ladi. Shifrlangan biletni *KDS2* serveri ochiq matn ko'rinishiga o'girib, bu bilet o'zlari bilan ishonchli hamkorlik qiluvchi Kerberos sohasi *KDS1* ning mijoziga berilganiga ishonch hosil qiladi. Bundan keyingi bajariladigan ishlar odatdagi Kerberos protokoli kabi bo'ladi.

§3.9. Elektron raqamli imzodan foydalanuvchi protokollar

Asimmetrik kriptosxemalardan foydalanuvchi «savol-javob» protokollarini 2 turga bo'lish mumkin:

1. Elektron raqamli imzo (ERI) dan foydalanuvchi protokollar;
2. Ochiq shifrlash sxemalaridan foydalanuvchi protokollar.

Elektron raqamli imzo va vaqt nishoniga asoslangan bir tomonlama autentifikasiyalash.

1. $P \rightarrow S: cert_A, t_A, V, S_A(t_A, V).$

Bu yerda $cert_A$ – foydalanuvchining ochiq kaliti sertifikat, t_A – vaqt nishoni, V – server identifikatori, S_A – foydalanuvchi imzosi. Imzo

birlari boshqasi ham k sirni bilishiga, ya'ni mo'ljallanayotgan huzukor «o'ziniki» ekanligiga ishonch hosil qilishlari lozim bo'ladi. Bunda abonentlarning hech qaysisi aloqa kanalini eshitishi mumkin bo'lgan nafaqat buzg'unchiga, balki «o'ziniki»ga ham k sirni ochishni istamaydilar.

Ushbu protokollarni qo'llanilishiga misol sifatida samoliyotlarni tanish tizimini ko'rsatish mumkin. A abonent sifatida samoliyot, B abonent sifatida baza ishtirok etishi mumkin. Baza tomonidan samoliyot payqalgan vaqtda o'zaro identifikasiyalashni amalga oshirish kerak. Agar «o'ziniki» bo'lsa, baza samoliyotni o'tkazib yuboradi. «Begona» bo'lsa, havo hududini buzayotganligi to'g'risida ogohlantirish beriladi. Xuddi shuningdek, samoliyot ham ko'rsatmalarni aynan «o'zining» bazasidan olayotganiga ishonch hosil qilishi lozim.

Shuningdek, «qo'l siqishish» protokollari «intellektual kartochka – «o'qish qurilmasi» tizimida ham o'zaro identifikasiyalashda qo'llaniladi. Bunung uchun abonentlar quyida keltirilgan 1-«qo'l siqishish» protokolidan foydalanishlari mumkin.

§3.12. 1-«qo'l siqishish» protokoli

$E_k(x)$ – k kalit bilan simmetrik kriptotizimdan foydalanib x matnini shifrlash, k – faqat «o'zlariniki» bo'lgan abonentlar biladigan maxfiy kalit bo'lsin.

Protokolni quyidagi sxematik tarzda amalga oshirish mumkin:

$A \rightarrow B$: tasodifiy r_1 sonini generasiya qilib, uni B abonentga jo'natadi.

$B \rightarrow A$: B abonent k kalitdan foydalanib r_1 ni shifrlaydi – $s_1 = E_k(r_1)$ va uni A abonentga jo'natadi.

A : $s_1 = E_k(r_1)$ ni hisoblaydi va $s_1 = s_1^*$ munosabatni tekshiradi. Agar bu munosabat o'rinli bo'lmasa, B abonentni «begona» sifatida qabul qiladi va protokol ishini to'xtatadi. Aks holda B abonentni «o'ziniki» deb biladi.

$B \rightarrow A$: tasodifiy r_2 sonini generasiya qilib, uni A abonentga jo'natadi.

$A \rightarrow B$: A abonent k kalitdan foydalanib r_2 ni shifrlaydi – $s_2 = E_k(r_2)$ va uni B abonentga jo'natadi.

Bu yerda $KA,otkr$; $KA,sekr$ - P foydalanuvchining mos holda ochiq va maxfiy kalitlari, $KS,otkr$; $KS,sekr$ - S serverning mos holda ochiq va maxfiy kalitlari, A - foydalanuvchining identifikatori, r_1, r_2 - mos holda foydalanuvchi va server tomonidan generasiya qilingan tasodifiy sonlar.

1-chi qadamda P foydalanuvchi r_1 tasodifiy sonni generasiya qiladi. Ushbu son bilan o'zining identifikatori A ni serverni ochiq kalitidan foydalanib, shifrlaydi va uni S serverga jo'natadi. Shifrlangan ma'lumotni qabul qilgan server o'zining maxfiy kaliti $KS,sekr$ bilan dastlabki matnga o'giradi va r_1 soniga ega bo'ladi.

2-chi qadamda server r_2 tasodifiy sonni generasiya qiladi. (r_1, r_2) juftlikni P foydalanuvchining ochiq kaliti $KA,otkr$ asosida shifrlab, foydalanuvchiga jo'natadi. Shifrlangan ma'lumotni qabul qilgan foydalanuvchi o'zining maxfiy kaliti $KA,sekr$ bilan dastlabki matnga o'giradi va o'zi jo'natgan r_1 sonini tiklaydi (shu sabab server autentifikasiyalashdan o'tdi) hamda r_2 sonini hosil qiladi.

3-qadamda foydalanuvchi r_2 sonini serverni o'ziga jo'natadi (shu bilan server tomonidan foydalanuvchi autentifikasiyalanadi) va tizimga kirish huquqiga ega bo'ladi.

§3.11. «Savol-javob» turidagi o'zaro identifikasiyalash protokollari

Savol-javob sxemalari o'zaro identifikasiyalashda qo'llaniladi. Identifika-siyalashdan o'tish uchun har bir ishtirokchi boshqasiga qandaydir ishonchli axborotni taqdim qiladi.

O'zaro identifikasiyalash har bir ishtirokchiga ma'lum bo'lgan umumiy sir asosida (bunday yondoshuv «o'zimizniki-begona» tizimlarida qo'llaniladi), Shuningdek, ishtirokchilar umumiy sirga ega bo'lmagan hollarda, ishtirokchilarning ochiq kalitlari saqlanadigan biron bir ishonchli markaz orqali amalga oshiriladi. «O'zimizniki-begona» tizimlaridan foydalanuvchi protokollar «qo'l siqishish» protokollari deb nomlanadi.

Faraz qilaylik A va B abonentlar bo'lsin. Ushbu abonentlarning har biri umumiy sir k ni (bu sirni biluvchilarni abonentlar «o'zimizniki», aks holda «begona» deb hisoblaydilar) biladilar. A va B abonentlar bir-biri bilan muomalaga kirishishmoqchi. Buning uchun, avvalo ularning har

abonentni A abonent identifikatsiyalashdan o'tkazadi. Bu holatda B abonent protokolning ikkinchi qismida identifikatsiyalashdan aynan A abonent o'tishiga ishonchi yo'q. Bu kamchilik quyida keltirilgan 2-«qo'l siqishish» protokolida bartaraf qilingan.

§3.13. 2-«qo'l siqishish» protokoli

1-«qo'l siqishish» protokolida foydalanilgan parametrlar bu yerda ham ishlatiladi: $E_k(x)$ – k kalit bilan simmetrik kriptotizimdan foydalanib x matni shifrlash, k – faqat «o'zlariniki» bo'lgan abonentlar biladigan maxfiy kalit.

Protokol quyidagi qadamlardan iborat:

$A \rightarrow B$: tasodifiy r_1 sonini generatsiya qilib, uni B abonentga jo'natadi.

$B \rightarrow A$: B abonent tasodifiy r_2 sonini generatsiya qiladi. k kalitdan foydalanib r_1 , r_2 va B^* ni shifrlaydi – $s_1 = E_k(r_1, r_2, B^*)$ va uni A abonentga jo'natadi (B^* – B abonentning identifikatori, shart bo'lmagan parametr).

A : $(r_1', r_2', B^*) = D_k(s_1)$ ni hisoblaydi va $r_1 = r_1'$ munosabatni tekshiradi. Agar bu munosabat o'rinli bo'lmasa, B abonentni «begona» sifatida qabul qiladi va protokol ishini to'xtatadi. Aks holda B abonentni «o'ziniki» deb biladi.

$B \rightarrow A$: tasodifiy r_2 sonini generatsiya qilib, uni A abonentga jo'natadi.

$A \rightarrow B$: A abonent k kalitdan foydalanib (r_2, r_1) juftlikni shifrlaydi – $s_2 = E_k(r_2, r_1)$ va uni B abonentga jo'natadi.

B : B abonent $(r_2', r_1') = D_k(s_2)$ ni hisoblaydi va $r_1 = r_1'$, $r_2 = r_2'$ munosabatlarni tekshiradi. Agar bu munosabatlar o'rinli bo'lmasa, A abonentni «begona» sifatida qabul qiladi va protokolni to'xtatadi. Aks holda A abonentni «o'ziniki» deb biladi.

Parametrlarni tanlash bo'yicha birinchi protokolda qo'yilgan talablar ushbu protokol uchun ham o'rinlidir.

2-«qo'l siqishish» protokolining yutug'i shundaki, bunda barcha qadamlar bir-biriga bog'langan. Shu sababli protokolni amalga oshirish jarayonida A va B abonentlar o'rtasidagi barcha xabarlarni qo'lga kiritgan buzg'unchi shifrlashning maxfiy k kalitini bilsagina, faqat shu holda parametrlarning qiymatlarini o'zgartirishi mumkin.

$B: s_2^* = E_k(r_2)$ ni hisoblaydi va $s_2 = s_2^*$ munosabatni tekshiradi. Agar bu munosabat o'rinli bo'lmasa, A abonentni «begona» sifatida qabul qiladi va protokolni to'xtatadi. Aks holda A abonentni «o'ziniki» deb biladi.

Ushbu protokolda maxfiy k kalit aloqa kanali bo'yicha jo'natilmaydi, faqatgina shifrlash kaliti sifatida ishlatiladi. Protokolning mustahkamligi protokolda foydalanilayotgan shifrlash tizimining kriptomustahkamligi bilan bog'liq. Agar shifrlash tizimi «ochiq matn – sifr matn» juftligi ma'lum bo'lgan hujumga nisbatan bardoshli bo'lsa, 2 ta qonuniy foydalanuvchilar aloqa kanalini eshitib boruvchi buzg'unchi yetarlicha ehtimollik bilan maxfiy k kalitni aniqlay olmaydi.

Agar bir xil matnni turli xil kalitlar bilan shifrlash natijasida har xil shifr matnlar hosil qilinsa, «o'ziniki» sifatida tutuvchi raqib s_i ($i=1,2$) parametrlarning to'g'ri qiymatlarini aniqlay olmaydi.

Agar E kriptotizim determinallashtirilgan bo'lsa (ya'ni, har bir (x,k) juftlikka faqatgina bitta y - shifrmavn mos kelsa), u holda maxfiy kalitga ega bo'lgan A va B qonuniy abonentlar har doim $s_1 = s_1^*$, $s_2 = s_2^*$ munosabatlarni bajarilishiga erishadilar. Demak, protokolni har bir amalga oshishida bir-birlarini «o'ziniki» sifatida aniqlaydilar.

Shunday qilib, ushbu protokolda foydalaniladigan kriptotizim simmetrik, determinallashtirilgan hamda «ochiq matn – sifr matn» juftligi asosidagi hujumga nisbatan bardoshli bo'lishi lozim.

Shuni ham qayd qilish lozimki, aloqa kanalini eshitib boruvchi buzg'unchi yoki raqib xabarlar uzatilayotganda r_i va s_i ($i=1,2$) parametrlarni qiymatlarini o'zgartirishi mumkin. Buning natijasida u A va B qonuniy abonentlarni bir-birlarini «begona» sifatida qabul qilishlariga erishadi.

r_i ($i=1,2$) parametrlarning qiymatlar tasodifiy bo'lishlari ham katta ahamiyatga ega. Bu parametrlarning qiymatlarini takroran ishlatmaslik zarur. Aks holda A va B qonuniy abonentlarni xabarlaridan r_i ($i=1,2$) parametrlarning bu qiymatlarini tutib olgan raqib boshqa safar bu qiymatlardan foydalanib, identifikasiyalashdan muvaffaqiyatli o'tishi mumkin.

Ushbu protokol yetarli darajada yaxshi emas, chunki u butunlik xossasini qanoatlantirmaydi. Haqiqatan ham, bu protokol bir-biriga bog'liq bo'lmagan 2 ta simmetrik mustaqil qismdan iborat. Birinchi qismida B

protokollarda isbot qiluvchi A abonent tekshiruvchi B abonentga o'zini parolini jo'natadi. Natijada B abonentda A abonent nomidan ish ko'rishga imkoniyat yaratiladi. Savol-javobga asoslangan protokollardan foydalanib ushbu kamchilikni yo'qotish mumkin. Ushbu protokollarni bajarilishida A abonent vaqt o'tishi bilan B abonentning savollariga javob berib boradi. Ammo, B abonentda A abonentdan olingan axborot natijasida keyinchalik A abonent nomidan ish yuritishiga axborot yetarli bo'lmaydi, ya'ni A abonent o'ziga tegishli bo'lgan sirni unchalik ahamiyatga ega bo'lmagan qismini beradi. Bu masala 4-bobning isboti nol oshkoralikka asoslangan autentifikasiyalash protokoli mavzusida bayon qilingan edi.

Ushu bobda oshkoraligi nol bo'lgan bir necha protokollar bayon etiladi. Oshkoraligi nol bo'lgan protokollarda sirni biluvchilarda sir haqida bilishini isbotlash imkoniyati mavjud. Ushbu protokollar ehtimollik xarakteriga ega bo'ladi, ya'ni isbotlovchi birga yaqin ehtimollik bilan sirni bilishini isbotlaydi.

Oshkoraligi nol bo'lgan protokollar (P, V, s) da P isbotlovchi (da'vogar) V tekshiruvchi (verifikator) ga s sir (tasdiq) ni bilishini isbotlaydi. Bunda abonent V mustaqil tarzda tekshirish imkoniga ega emas va u raqib ham emas deb faraz qilinadi. Abonent B esa yolg'on tasdiqni rostligini isbotlashga urinadigan raqib ham bo'lishi mumkin. P va V abonentlar o'rtasida axborot almashinuviga asoslangan va bir necha raunddan iborat bo'lgan oshkoraligi nol bo'lgan protokollar quyidagi 3 ta shartni qanoatlantirishi lozim:

– *to'liqlik*, ya'ni agar s tasdiq haqiqatan ham rost bo'lsa, u holda isbotlovchi tekshiruvchini buni tan olishiga ishontirishi lozim;

– *korrektilik*, ya'ni agar s tasdiq yolg'on bo'lsa, u holda isbotlovchi tekshiruvchini tasdiqni aksiga ishontirovmasligi lozim;

– *nolli oshkoralik*, protokolni amalga oshirish natijasida abonent V tasdiq s haqida o'z bilimlarini oshirmasligi lozim. Boshqacha aytganda, abonent P qandaydir maxfiy axborotga ega ekanligini abonent V ga uni mohiyatini oshkor qilmasdan isbotlashi kerak bo'ladi.

Oshkoraligi nol bo'lgan protokollarni quyidagicha talqin qilish mumkin. Isbot qiluvchi P abonent oldindan kelishilgan oraliqdagi tasodifiy elementni protokolda o'zining maxfiy kaliti sifatida foydalanish uchun tanlaydi. Maxfiy kalitini qandaydir bir tomonlama funksiyaning argumenti

4-BOB. ISBOTI NOL OSHKORALIKKA ASOSLANGAN AUTENTIFIKASIYALASH PROTOKOLLARI

Isboti nol oshkoralikka asoslangan autentifikasiyalash protokollarini amalga oshirish uchun barcha abonentlar ishonchiga ega bo'lgan ishonchli markaz xizmatidan foydalaniladi. Bu ishonchli markazda barcha abonentlarning ochiq kalitlari ularning identifikatori bilan birgalikda saqlanadi.

Ixtiyoriy isboti nol oshkoralikka asoslangan autentifikasiyalash protokollari quyidagi prinsip asosida amalga oshiriladi: ochiq va yopiq kalitlar juftligiga ega bo'lgan P qonuniy foydalanuvchi va V tekshiruvchi protokolni birgalikda bajaradilar. Ushbu protokolda P foydalanuvchi o'zining yopiq kalitini bilishini namoyish qilish orqali o'zining haqiqiylikini isbotlaydi [3,10]. Bunda u yopiq kaliti (yoki maxfiy axborot) ni oshkor qilmasligi lozim bo'ladi (V tekshiruvchi P foydalanuvchidan olgan axborotlari asosida uning yopiq kalitini hisoblab topishi mumkin bo'lmasligi kerak). Ushbu turdagi protokollar 2 bosqich – tayyorgarlik va ishchi bosqichlarida amalga oshiriladi.

Tayyorgarlik bosqichida protokolda foydalaniladigan ayrim parametrlar va ularning qiymatlari (jumladan, foydalanuvchi ochiq va yopiq kalitlari) hosil qilinadi.

Ishchi bosqichida foydalanuvchini autentifikasiyalash amalga oshiriladi, boshqacha aytganda, foydalanuvchini autentligi isbotlanadi.

§4.1. Oshkoraligi nol bo'lgan protokollar

Kriptografik amaliyotda shunday hollar ham uchraydiki, bu hollarda bir abonent ikkinchi abonentga biror sirni bilishini ayrim yo'llar bilan isbotlaydi (yoki tasdiqlaydi) va bu isbotlash natijasida sirni teksiruvchii, ya'ni ikkinchi abonent sir haqida ma'lumotga ega bo'lmaydi. Masalan, Alisa biror murakkab masalani yechimini biladi. U yechimni bilishi haqida Bobni shunday ishontiradiki, natijada Bob masalani yechimi haqida o'zi bilgan axborot va Alisadan olgan qo'shimcha axborotlardan foydalanib, masalani yechish imkoniyatiga ega bo'lmaydi. Bir qarashda ushbu ishni amalga oshirish mumkin emasga o'xshaydi. Ammo, bu ishni ayrim kriptografik amallardan foydalanib, uddalash mimkin. Bunday masalalar, kompyuter tarmoqlari ichun ham ahamiyatlidir. Masalan, parolli

§4.2. Ali Bobo g'ori nollı oshkoralikka misol sifatida

Ushbu paragrafda Ali Bobo g'ori misolida nol oshkoralik bilan isbotlash protokolini fizik amalga oshirish ko'rib chiqiladi. G'orning ichida D eshik mavjud. Protokolning P ishtirokchisida D eshikni ochishning maxfiy kaliti bor. P ishtirokchi o'zining eshikdan o'tish qobiliyatini (y' ani, unda maxfiy kalitni mavjudligini) eshikdan o'tishni ko'rsatmasdan tirib V tekshiruvchiga isbotlashni xohlaydi.

Ushbu protokolni quyidagicha amalga oshirish mumkin:

1. P ishtirokchi g'orni ichiga kiradi va D eshikka D' yoki D'' ixtiyoriy tomondan yaqinlashadiki, natijada V tekshiruvchi uni eshikni qaysi tomonida turganligini bilmaydi.

2. V tekshiruvchi g'orni ichiga kiradi va P ishtirokchidan g'orning biror (chap yoki o'ng) tomonidan chiqishni so'raydi.

3. P ishtirokchi o'zidagi maxfiy kalitdan foydalanib, g'orning ixtiyoriy tomonida paydo bo'lish orqali V tekshiruvchini istagini ruyobga chiqarishi mumkin.

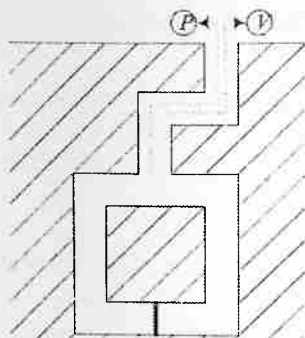
4.1-rasmda ushbu protokolni fizik amalga oshirishning sxematik ko'rinishi keltirilgan. Protokolning ayrim qadamlarida psevido tasodifiy sonlar generatori sifatida ishtirokchilar tomonidan tanga tashlash prosedurasi ishlatilgan.

Ko'rinib turibdiki, g'orning V tekshiruvchi ko'rsatgan tomonidan P isbot qiluvchining xuddi shu tarzda k marta muvaffaqiyatli chiqib kelishi natijasida P isbot qiluvchining V tekshiruvchini aldash ehtimoli $1/2^k$ ga teng bo'ladi. Bu holat esa k ning qiymati oshgani sari P isbot qiluvchida haqiqatan ham g'orning D eshigini ochishning maxfiy kaliti borligiga V tekshiruvchining ishonchi ortib borishiga sababchi bo'ladi.

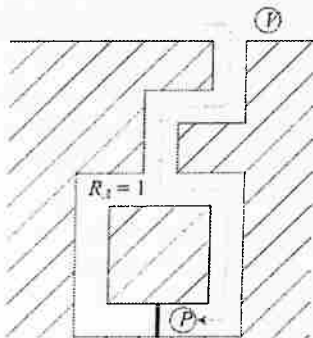
P isbot qiluvchi va V tekshiruvchi dastlabki holatga, ya'ni A nuqtaga qaytishadi. $7/8$ ehtimollik bilan tasdiqlash mumkinki, P isbot qiluvchi D eshikdan o'tish sirini biladi.

sifatida foydalanib, ushbu bir tomonlama funksiyani qiymatini hisoblab, tekshiruvchiga taqdim qiladi. Bu bilan protokoldagi turli iteratsiyalarning tasodifiyligi va bog'liqsizligi ta'minlanadi hamda isbot qiluvchi P abonent har biriga javob berishga tayyor bo'lgan savollar habori aniqlanadi. Oshkoraligi nol bo'lgan protokollar shunday quriladiki, s sirga ega bo'lgan P isbot qiluvchigina barcha savollarga javob berishi mumkin va bu barcha javoblar s sir haqida axborot bermaydi. Keyingi bosqichda V tekshiruvchi bu savollardan birini isbot qiluvchi P abonentga beradi. P abonentning bu savolga bergan javobi V tekshiruvchi tomonidan tekshiriladi. Isbot qiluvchi P abonentning g'irromligiga yo'l qo'ymaslik maqsadida bu protokol zarur iteratsiya sonigacha bajariladi.

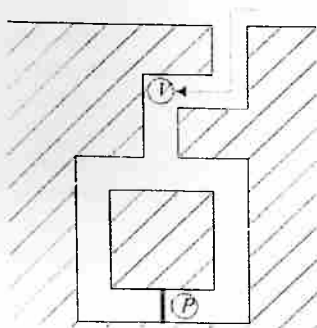
Nolli oshkoralik, ayniqsa, autentifikasiyalash protokollarini amalga oshirishda katta ahamiyatga ega. Masalan, P – bank mijozlari kartochkalarida o'rnatilgan algoritim (A abonent), V esa bank kompyuterida bajariladigan dastur (B abonent) bo'lsin. Kartochkadan foydalanib, har qanday haridni amalga oshirishdan oldin bank kartochkaning haqiqiylikiga ishonch hosil qilishi va uning egasini identifikasiyalashi lozim bo'ladi. Bu maqsadda (P, V, s) protokolidan foydalanilsa, protokolning to'liqlik xossasi kartochkaga o'zining autentligini isbotlash; korrektlik xossasi esa qalbaki kartochkadan foydalanishga uringan buzg'inchining harakatidan bankni manfaatini himoyalash; nolli oshkoralik xossasi autentifikasiyalashning oldingi raundlarida tutib olingan axborotlar asosida A abonent nomidan autentifikasiyalashdan o'tmoqchi bo'lgan buzg'inchidan mijozni himoyalash imkononi beradi.



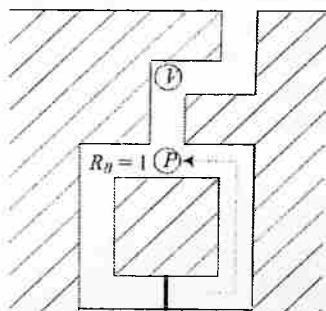
P isbot qiluvchi va V tekshiruvchi dastlabki holatga, ya'ni A nuqtaga qaytishadi.



P isbot qiluvchi g' orga tushmoqda. C nuqtaga yetganda tanga tashlaydi: natija $R_A=1$, shu bois u o'ngga burilib, D'' nuqtagacha tushib keladi. V tekshiruvchi P isbot qiluvchini qayerdaligini ko'rmaydi.

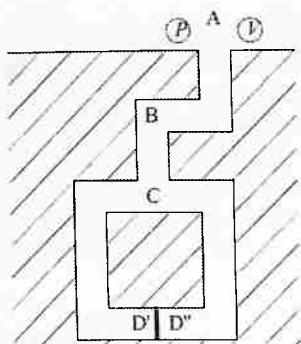


V tekshiruvchi B nuqtagacha tushib keladi, V tekshiruvchi P isbot qiluvchi qayerda turganligini ko'rmaydi.

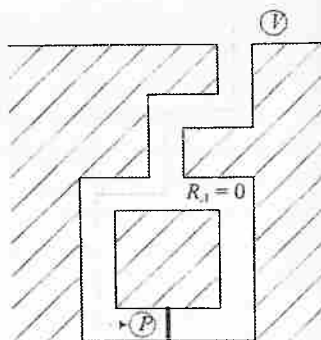


V tekshiruvchi B nuqtada tanga tashlaydi: natija $R_B=1$. Shu sababli u P isbot qiluvchidan g' orning o'ng tomonidan chiqishini so'raydi. P isbot qiluvchi eshikdan o'tishiga hojat qolmaydi, D'' nuqtadan B nuqtaga qaytadi.

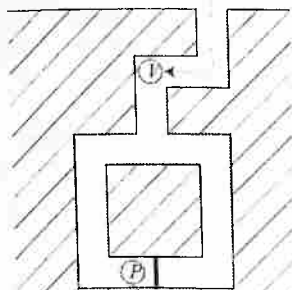
4.1-rasm. Nol oshkoralik g' ori.



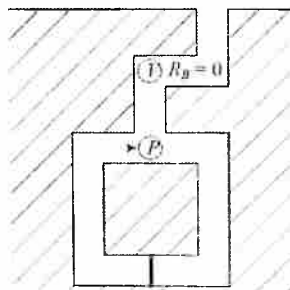
Dastlabki holat.
P isbot qiluvchi va *V* tekshiruvchi
A nuqtada turishibdi.



P isbot qiluvchi g'orga tushib kelmoqda. *C* nuqtaga yetganda tanga tashlaydi: natija $R_A=0$, shu sababli u chapga burilib, *D'* nuqtagacha nushib keladi. *V* tekshiruvchi *P* isbot qiluvchi qayerga burilganligini ko'rmaydi.



V tekshiruvchi *B* nuqtagacha tushib keladi. *V* tekshiruvchi *P* isbot qiluvchi qayerda turganligini ko'rmaydi.



V tekshiruvchi *B* nuqtada tanga tashlaydi: natija $R_B=0$. Shu sababli u *P* isbot qiluvchidan g'orning chap tomonidan chiqish-ni so'raydi. *P* isbot qiluvchi eshikdan o'tishiga hojat qolmaydi, *D'* nuqtadan *B* nuqtaga qaytadi.

b bitning qiymatiga bog'liq holda $y^2 \equiv x(\text{mod } n)$ yoki $y^2 \equiv x \cdot v(\text{mod } n)$ shartlardan biri bajarilishini payqash mumkin.

Ushbu protokolni korrektiligini quyida keltirilgan mulohazalar bilan asoslash mumkin.

b bitdan foydalanish P abonentga nisbatan quyida keltirilgan ikkita talabni amalga oshirish uchun ishlatilgan:

- 1) s sirni bilishini namoyish qilish;
- 2) yolg'on javob berishini oldini olish maqsadida.

O'zini P abonent sifatida tutuvchi raqib ixtiyoriy z sonini tanlab, V tekshiruvchiga $x = z^2/v$ sonini jo'natish orqali V tekshiruvchini aldasha harakat qilishi mumkin. U holda u $b=1$ bo'lganda $y = z$ to'g'ri javobni tekshiruvchiga jo'natishi mumkin. Ammo, $b=0$ bo'lganda u javob berolmaydi. Bunga javob berish x sonidan n modul bo'yocha kvadrat ildiz chiqarishni talab qiladi. Buni esa hozirgi kunda amalga oshirishning imkoni yo'q.

s sirni biluvchi P abonent ikkita savolga ham javob berish imkoniyatiga ega. Agar s sirni bilmasa eng yaxshi holda u ikkita savoldan bittasiga javob berish mumkin. Shunday qilib, aldash $1/2$ dan katta bo'lmagan ehtimollik bilan bajariladi. t ga karrali iteratsiyali protokolda aldovni sodir bo'lish ehtimoli 2^{-t} miqdordan oshmaydi. Shu sababli ushbu protokolda iteratsiyalar soni t ni $20 \leq t \leq 40$ oraliqdan tanlash tavsiya etiladi.

$y = z$ javob isbot qiluvchi P abonentning s siriga bog'liq emas. $y = z \cdot s \text{ mod } n$ javobda s sir haqida ma'lumot yo'q. Chunki tasodifiy z sonini V tekshiruvchi bilmaydi va bilish imkoniyatiga ham ega emas.

Protokolni ayrim jihatlarini tahlil qilish maqsadga muvofiq. 2-chi qadamdagi bit b ni jo'natishdagi so'rovnomada 2 ta maqsad e'tiborga olingan. Bu maqsadlarning birinchisi foydalanuvchi maxfiy s kalitni bilishini namoyish qilishidan iborat. Ikkinchisi halol foydalanuvchini g'irrom tekshiruvchi aldovidan himoya qilishdir. 3-chi qadamda so'rovnomaga foydalanuvchi tekshiruvchiga $y = r$ yoki $y \equiv r \cdot s(\text{mod } n)$ bilan javob qaytaradi. Bu javoblarning birontasida maxfiy s kalit haqida biron bir axborot yo'q. Birinchi javob maxfiy s kalitga umuman bog'liq

§4.3. Fiat – Shamirning autentifikasiyalash protokoli

Ushbu protokolda isbot qiluvchi P abonent tekshiruvchi V abonentga s sirni bilishini 3 ta qadamga asoslangan t iterasiya yordamida isbotlaydi. Protokol katta son n ning moduli bo'yicha kvadrat ildiz chiqarishning murakkabligiga asoslangan. Shu sababli bu masala n sonini tub ko'paytuvchilarga yoyish masalasi bilan ekvivalent.

Qandaydir T ishonchli markaz 2 ta katta p va q tub sonlarini tanlaydi. $N=pq$ modulni hisoblaydi va uni barcha isbotlovchilarga tarqatadi (yoki e'lon qiladi). Ammo, bunda p va q sonlarini sirligi saqlanib qolinadi.

Har bir isbot qiluvchi P abonent n soniga o'zaro tub bo'lgan s sonni quyidagi shart asosida tasodifiy tanlaydi va v miqdorni hisoblaydi:

$$1 \leq s \leq n-1,$$

$$v = s^2 \bmod n.$$

v ni o'zining ochiq kaliti sifatida e'lon qiladi. s esa abonentning maxfiy kaliti hisoblanadi.

Protokolda quyida keltirigan 3 ta qadam bir-biriga bog'liq bo'lmagan holda t marta amalga oshiriladi. Agar barcha iterasiyalar ijobiy natijaga olib kelsa, u holda V abonent haqiqatdan ham P abonent s sirni bilishini isbotini qabul qiladi.

Protokolda amalga oshiriladigan qadamlar quyidagilardan iborat:

1) P abonent $1 < z < n-1$ oraliqdan tasodifiy z sonini tanlaydi va V tekshiruvchiga $x = z^2 \bmod n$ sonini jo'natadi.

2) V tekshiruvchi tasodifiy $b \in \{0,1\}$ bitni tanlaydi va uni P abonentga jo'natadi.

3) P abonent y sonini hisoblab, uni V tekshiruvchiga jo'natadi. Bu yerda y sonini qiymati b bitning qiymatiga bog'liq bo'ladi: agar $b=0$ bo'lsa, $y=z$ bo'ladi; agar $b=1$ bo'lsa, $y=z \cdot s \bmod n$ bo'ladi. V tekshiruvchi y sonini qiymatiga bog'liq holda qaror qabul qiladi: agar $y \neq 0$ yoki $y^2 \equiv x \cdot v^b \pmod{n}$ o'rinli bo'lsa, V tekshiruvchi ijobiy qaror qabul qiladi.

§4.4. Autentifikasiyalashning Shnorrx sxemasi

Shnorrx protokoli

$$y = \alpha^x \pmod{p}$$

berilgan qiymatga ko'ra, $x \in Z_q$ sonni topishning samarali algoritmi mavjud emasligiga asoslangan. Shnorrx sxemasining nolli oshkoralik xossasi hozircha isbotlanmagan. Shunday bo'lsa-da, hozirgi vaqtda Shnorrx protokoli autentifikasiyalashning eng samarali protokollaridan biri sifatida e'tirof etiladi.

Bu protokolda ham o'zining ochiq va yopiq kalitlariga ega bo'lgan ishonchli markaz xizmatidan foydalaniladi.

Tayyorgarlik bosqichida ishonchli markaz quyidagi parametrlarni tanlaydi va barcha abonentlarga e'lon qiladi:

p, q – tub sonlar. q soni $p-1$ sonining tub bo'luvchisi. Shnorrx p soninig razriyadini 512 bitdan, q soninig razriyadini esa 140 bitdan kam bo'lmasligini taklif qilgan;

$\alpha - Z_p$ maydon elementi bo'lib, uning tartibi q sonining tartibiga teng (ya'ni, $\alpha^q = 1 \pmod{p}$, $\alpha \neq 1$);

$t \in N - q > 2^t$ shartni qanoatlantiruvchi xavfsizlik parametri.

Autentligini isbot qiluvchi P abonent quyidagi parametrlarga ega:

$s \in Z_q$ – abonentning yopiq kaliti;

$v = \alpha^s \pmod{p}$ – abonentning ochiq kaliti.

Ishonchli markazda qayddan o'tish uchun har bir abonent o'zining identifikatori I ni markazga taqdim qilishi lozim. Shundan so'ngina ishonchli markaz (I, v) juftlikni imzolaydi.

Ishchi bosqichi quyidagicha amalga oshiriladi:

1. $P \rightarrow V: x = \alpha^r \pmod{p}$, bu yerda $r \in Z_q$ – tasodifiy son.

2. $V \rightarrow P: 1 \leq e \leq 2^t$, bu yerda e – tasodifiy son.

3. $P \rightarrow V: y = (r + se) \pmod{q}$.

Ishchi bosqichi qadamlarini quyidagicha izohlash mumkin.

Isbot qiluvchi P abonent $1 \leq r \leq q-1$ kesmadan r sonini tasodifiy tanlaydi va tekshiruvchi V ga $x = \alpha^r \pmod{p}$ sonni jo'natadi.

emas. Ikkinchi javobda esa bu kalit faqatgina foydalanuvchiga ma'lum bo'lgan tasodifiy r soni bilan niqoblangan.

Foydalanuvchi nomidan ish ko'ruvchi buzg'unchi tekshiruvchini aldashga harakat qilishi mumkin: buning uchun u ixtiyoriy r sonini tanlab,

$x = \frac{r^2}{v} \pmod{n}$ ni hisoblab, $b=0$ bo'lsa, tekshiruvchiga $y=r$ ni jo'natish

mumkin. Ammo, $b=1$ bo'lganda, u javob bera olmaydi, buning uchun u $\sqrt{x} \pmod{n}$ bilishi lozim bo'ladi. Ko'rinib turibdiki, protokol haqiqatan ham nol oshkorlik xususiyatiga ega ekan.

Misol. T ishonchli markaz p va q tub sonlarini $p=23$ va $q=19$ tarzda tanlab, $n=pq=23 \cdot 19=437$ ni e'lon qiladi.

Isbot qiluvchi P abonent n soniga o'zaro tub bo'lgan s sirni (ya'ni, maxfiy kalitni) $1 \leq s \leq n-1$ oraliqdan $s=436$ sifatida tanlaydi hamda ochiq kaliti v ni hisoblaydi:

$$v = s^2 \pmod{n} = 436^2 \pmod{437} = 190096 \pmod{437} = 1.$$

Protokol quyidagicha amalga oshiriladi:

1) P abonent $1 < z < n-1$ oraliqdan tasodifiy $z=50$ sonini tanlaydi va V tekshiruvchiga $x=z^2 \pmod{n} = 50^2 \pmod{437} = 2500 \pmod{437} = 315 \pmod{437}$ sonini jo'natadi.

2) V tekshiruvchi tasodifiy $b \in \{0,1\}$ bitni tanlaydi va uni P abonentga jo'natadi.

3) P abonent $b=0$ bo'lsa, $y=z=50$ sonini, $b=1$ bo'lsa,

$$y = z \cdot s \pmod{n} = 50 \cdot 436 \pmod{437} = 387$$

sonini hisoblab, V tekshiruvchiga jo'natadi.

$y \neq 0$ tengsizlik o'rinli ekanligi ko'rinib turibdi. Shu sababli, V tekshiruvchi $y^2 \equiv x \cdot v^b \pmod{n}$ taqqoslamani tekshirib ko'radi:

$$50^2 \equiv 315 \cdot 1^1 \pmod{437} = 315 \pmod{437}.$$

Bu taqqoslamani o'rinli ekanligi protokolning 1-qadamidan ham ko'rinib turibdi. Shu bois, V tekshiruvchi bu iteratsiyada ijobiy qaror qabul qiladi. Shu tarzda bir necha iteratsiya bajariladi va barcha iteratsiyalarning natijalari ijobiy bo'lsa, V tekshiruvchi haqiqatdan ham P abonent s sirni bilishini isbotini qabul qiladi.

$v = \alpha^{-3} \pmod p$ – abonentning ochiq kaliti.

Brikell va MakKarli protokolining ishchi bosqichi Shnor protokolidagi qadamlarni aynan takrorlashdan iborat. Faqatgina p va q tub sonlarini tanlash sharti bilan Brikell va MakKarli sxemasi Shnor sxemasidan farqlanadi. Brikell va MakKarli sxemasida $p-1$ soni 2 ta - q va w katta tub bo'luvchilarga ega.

Uchbu protokolning to'liqlik va korrektlik xossalari Shnor protokolidagi kabi izohlanadi.

§4.6. Gillu-Kiskate protokoli

Ishonchli markaz tayyorgarlik bosqichida quyidagi parametrlarni tanlaydi:

$n = pq$ – RSA kriptotizimidagi modul;

b – tub son bo'lib, xavfsizlik parametri vazifasini bajaradi. Bu son $EKUB(b, \varphi(n)) = 1$ sharti bo'yicha tanlanadi.

n , b sonlari ochiq parametrlar sifatida abonentlarga e'lon qilinadi. p , q katta tub sonlari RSA kriptotizimidagi kabi maxfiy tutiladi.

P abonent quyidagi parametrlarni generasiya qiladi:

$s \in Z_q$ ($EKUB(s, n) = 1$) soni – abonentning yopiq kaliti;

$v = s^{-b} \pmod n$ – abonentning ochiq kaliti.

Protokolning ishchi bosqichi quyidagi qadamlardan iborat:

1. $P \rightarrow V$: $x = r^b \pmod n$, bu yerda $r \in Z_n$ – tasodifiy son;
2. $V \rightarrow P$: e , bu yerda e $1 \leq e \leq b-1$ kesmadan olingan tasodifiy son;
3. $P \rightarrow V$: $y = r s^e \pmod n$.

V tekshiruvchi

$$x \equiv y^b v^e \pmod n$$

taqqoslamani tekshirib ko'radi. Agar bu taqqoslama o'rinli bo'lsa, P abonentning isbotini qabul qiladi. Aks holda rad qiladi.

Protokolning to'liqligi. P abonent haqiqiy foydalanuvchi bo'lsa, u holda V tekshiruvchi tomonidan tekshiriladigan taqqoslama o'rinli bo'ladi. Haqiqatan ham

$$y^b v^e \equiv r^b s^{eb} v^e \equiv r^b s^{eb} s^{-eb} \equiv r^b \equiv x \pmod n.$$

V tekshiruvchi $1 \leq e < 2^l$ shart asosida tasodifiy tanlangan e sonini isbot qiluvchi P abonentga jo'natadi.

Isbot qiluvchi P abonent $y = (r + se) \bmod q$ sonni jo'natish orqali V tekshiruvchiga javob qaytaradi. Agar

$$x \equiv \alpha^y v^e \pmod{p}$$

taqqoslama o'rinli bo'lsa, V tekshiruvchi P abonentning isbotini qabul qiladi, aks holda rad qiladi.

Protokolning to'liqligi. Ushbu holatda protokolning to'liqligi isbot haqiqiy abonentdan olinganligi bilan, ya'ni

$$\alpha^y v^e \equiv \alpha^{r+se} \alpha^{-se} \equiv \alpha^{r+se-se} \equiv \alpha^r \equiv x \pmod{p}$$

taqqoslamaning o'rinli ekanligi bilan izohlanadi.

Protokolning korrektiligi. Ushbu holda protokolning korrektiligi haqiqiy abonent nomidan ish yurituvchi raqib yoki buzg'unchi tomonidan katta ehtimollik bilan isbotni taqdim qilinmaganligi bilan xarakterlanadi.

Shuni qayd qilish lozimki, protokolning ikkinchi qadamida tasodifiy e soni o'rniga $e \in \{0,1\}$ tasodifiy bitdan foydalanish mumkin. U holda protokolni amalga oshirish uchun yuqorida keltirilgan uch qadamli ishchi bosqichni bir necha marta takrorlash talab etiladi.

§4.5. Autentifikasiyalashning Brikell va MakKarli sxemasi

Ushbu protokolda ishonchli markaz tayyorgarlik bosqichida quyidagi parametrlarni tanlaydi:

$k \approx 140$ – parametr;

p, q va w – tub sonlar. qw ko'paytma $(p-1)$ ning bo'luvchisi bo'lib, q^2 esa $(p-1)$ ning bo'luvchisi emas. $q, w \geq 2^k$ va $p \geq 2^{512}$ shartlar asosida q, w va p tub sonlari tanlanadi;

$\alpha \in Z_p$ maydon elementi bo'lib, uning tartibi q sonining tartibiga teng (ya'ni, $\alpha^q = 1 \pmod{p}$, $\alpha \neq 1$);

p va α sonlarining qiymatlari e'lon qilinadi, q va w sonlari maxfiy tutiladi.

Autentligini isbot qiluvchi P abonent quyidagi parametrlarga ega:
 $s \in Z_q$ – abonentning yopiq kaliti;

$$\alpha_1^{y_1} \alpha_2^{y_2} v^e \equiv \alpha_1^{(r_1+s_1e)} \alpha_2^{(r_2+s_2e)} (\alpha_1^{-s_1})^e (\alpha_2^{-s_2})^e \equiv \alpha_1^{r_1} \alpha_2^{r_2} = x \pmod{p}.$$

Protokolning korrektiligi. Protokolning korrektiligi haqiqiy abonent nomidan ish yurituvchi raqib yoki buzg'unchi tomonidan katta ehtimollik bilan isbotni olinmaganligi bilan xarakterlanadi.

§4.8. Feige-Fiat-Shamir protokoli

Ushbu protokol Fiat-Shamir protokolining o'zgartirilgan varianti bo'lib, unda maxfiy va ochiq kalitlar vektorlaridan foydalaniladi.

Qandaydir T ishonchli markaz $n=pq$ modulni hisoblaydi va uni barcha isbotlovchilarga e'lon qiladi. Ammo, bunda p va q katta tub sonlarini sirligi saqlanib qolinadi. Amaliyotga qo'llash uchun n soni uzunligi 512 bitdan kam bo'lmasligi, ya'ni 1024 bitga yaqinroq bo'lishi lozim.

Isbot qiluvchi P abonent $S = [s_1, s_2, \dots, s_m]$ vektorni har bir elementi s_i ($i = \overline{1, m}$) ni n soniga o'zaro tublik shartidan foydalanib, $[1, n-1]$ kesmadan tasodifiy shakllantiradi. S vektori abonentning maxfiy kaliti hisoblanadi.

P abonentning S vektoriga mos keluvchi uning ochiq kaliti – $v = [v_1, v_2, \dots, v_m]$ vektor elementlari quyidagi munosabatdan foydalanib, aniqlanadi:

$$v_i = (s_i^2)^{-1} \pmod{n}, \quad (i = \overline{1, m}).$$

2-qadamdagi $B = [b_1, b_2, \dots, b_m]$ bitlar vektori tasodifiy tanlanadi.

Protokolda amalga oshiriladigan qadamlar:

1. P abonent $(1, n-1)$ oraliqdan tasodifiy z sonini tanlaydi va V tekshiruvchiga $x = z^2 \pmod{n}$ sonini jo'natadi.

2. V tekshiruvchi $B = [b_1, b_2, \dots, b_m]$ bitlar vektorini tasodifiy tanlaydi va uni P abonentga jo'natadi.

3. P abonent $y = (z \cdot s_1^{b_1} \cdot s_2^{b_2} \cdot \dots \cdot s_m^{b_m}) \pmod{n}$ sonini hisoblab, uni V tekshiruvchiga jo'natadi.

Protokolning korrektiligi. Protokolning korrektiligi haqiqiy abonent nomidan ish yurituvchi raqib yoki buzg'unchi tomonidan katta ehtimollik bilan isbotni tqadim qillinmaganligi bilan xarakterlanadi.

§4.7. Okamoto protokoli

Tayyorgarlik bosqichida ishonchli markaz quyidagi parametrlarni tanlaydi:

p, q – katta tub sonlar. q soni $p-1$ ning bo'luvchisidir.

$\alpha_1, \alpha_2 \in \mathbb{Z}_p - \mathbb{Z}_p$ maydon elementlari bo'lib, ularning tartibi q soniniki bilan bir xil, ya'ni, $\alpha_1^q = 1 \pmod{p}$, $\alpha_2^q = 1 \pmod{p}$ (bu yerda $\alpha_1, \alpha_2 \neq 1$);

$t \in \mathbb{N}$ – xavfsizlik parametri bo'lib, bu son $q > 2^t$ shartni qanoatlantiradi.

Shu bilan birgalikda ishonchli markazning o'zi ham ochiq va yopiq kalitlarga ega.

Isbotlovchi P abonent quyidagi parametrlarga ega:

$s_1, s_2 \in \mathbb{Z}_q - \mathbb{Z}_q$ maydon elementlari bo'lib, abonentning yopiq kalitlar juftligi sifatida abonent tomonidan maxfiy tutiladi.

$v = \alpha_1^{-s_1} \cdot \alpha_2^{-s_2} \pmod{p}$ – abonentning ochiq kalitlari hisoblanadi.

Ishonchli markazda qayddan o'tish uchun har bir abonent o'zining identifikatori I ni ishonchli markazga taqdim qilgandan so'ngina ishonchli markaz (I, v) juftlikni imzolaydi.

Protokolning ishchi bosqichi quyidagicha amalga oshiriladi:

- $P \rightarrow V: x = \alpha_1^{r_1} \alpha_2^{r_2} \pmod{p}$, bu yerda $r_1, r_2 \in \mathbb{Z}_q^*$ – tasodifiy sonlar;
- $V \rightarrow P: e$, bu yerda e $1 \leq e \leq 2^t$ shartni qanoatlantiruvchi tasodifiy son;
- $P \rightarrow V: y_1 = (r_1 + s_1 e) \pmod{q}$, $y_2 = (r_2 + s_2 e) \pmod{q}$.

V tekshiruvchi

$$x \equiv \alpha_1^{y_1} \alpha_2^{y_2} v^e \pmod{p}$$

taqqoslamani tekshirib ko'radi. Agar bu taqqoslama o'rinli bo'lsa, P abonentning isbotini qabul qiladi. Aks holda rad qiladi.

Protokolning to'liqligi. P abonent haqiqiy foydalanuvchi bo'lsa, u holda V tekshiruvchi tomonidan tekshiriladigan taqqoslama o'rinli bo'ladi. Haqiqatan ham

V tekshiruvchi tomonidan $(y^2 \cdot v_1^{b_1} \cdot v_2^{b_2} \cdot \dots \cdot v_m^{b_m}) \bmod n = x$ tenglik, ya'ni $(31^2 \cdot 4^1 \cdot 11^1 \cdot 16^0 \cdot 29) \bmod 35 = 11$, $1226236 \bmod 35 = 11$ yoki $11 = 11$ tenglikni bajarilishi tekshirib ko'riladi.

V tekshiruvchi butunlay ishonch hosil qilishi uchun ushbu protokol t marta takrorlanadi.

§4.9. RSA kriptotizimiga asoslangan protokol

Ma'lumki, RSA kriptotizimi hozirgi kunda amaliyotga keng qo'llanilayotgan kriptografik algoritmlardan biridir. Shu sababli RSA kriptotizimiga asoslangan, oshkoraligi nol bo'lgan protokollardan foydalanish katta amaliy ahamiyatga ega. Ushbu protokolda isbot qiluvchi abonent vazifasini Alisa bajaradi, tekshiruvchi sifatida Bob ishtirok etadi.

Faraz qilaylik, Alisa qanaqadir yo'llar bilan Mellorining yopiq kaliti d ni qo'lga kiritdi. U Bobga ushbu yopiq kalitni ko'rsatmasdan (ochmasdan) Bobni bunga ishontirishni xohlaydi. Agar Alisa o'z maqsadini amalga oshirish uchun Bobga qandaydir m matnini va unga mos keluvchi $s = m^d \bmod n$ imzoni ko'rsatsa, Bob $m = s^e \bmod n$ hisoblashni amalga oshirib, bu da'voni osongina tekshirib, imzoni to'g'riligiga ishonch hosil qilish mumkin. Ammo, Bob ko'rsatilgan matnini imzosini (Mellorining yopiq kalitini emas) Alisa qanaqadir yo'llar bilan qo'lga kiritgan degan shubhaga borishi mumkin.

Bob tasodifiy R sonini tanlab, bu sonni imzolash uchun Alisaga jo'natib, agar Alisa ushbu songa mos keluvchi imzoni Bobga taqdim qilsa, Bob Alisaning da'vosi to'g'ri ekanligiga ishonch hosil qilishi mumkin. Ammo, bu holda Alisa Bob maxsus tuzilmaga ega bo'lgan tasodifiy sonni jo'natib, unga mos keluvchi imzodan foydalanib, Mellorining maxfiy xatini Bob o'qishi mumkin degan xavotirga tushadi. Bu esa Mellorining yopiq kaliti d ga bo'lgan qiziqish so'nishiga olib keladi. Haqiqatan ham, C kriptogrammadagi axborotga ega bo'lish uchun n soniga o'zaro tub bo'lgan qandaydir t soni tanlanadi. Shuningdek, t soniga teskari qiymat $t^{-1}(\bmod n)$ va $t^e \bmod n$ hamda $m' = Ct^e(\bmod n)$ qiymatlar hisoblanadi.

V tekshiruvchi tomonidan $(y^2 \cdot v_1^{b_1} \cdot v_2^{b_2} \cdot \dots \cdot v_m^{b_m}) \bmod n = x$ tenglik tekshirib ko'riladi. Tenglik bajarilsa, V tekshiruvchi bu iteratsiyada ijobiy qaror qabul qiladi.

P abonent qonuniy isbot qiluvchi bo'lsa, u holda u 3-qadamda y sonini to'g'ri hisoblaydi. Natijada V tekshiruvchi tomonidan $(y^2 \cdot v_1^{b_1} \cdot v_2^{b_2} \cdot \dots \cdot v_m^{b_m}) \bmod n$ va x sonlarining tengligi tasdiqlanadi:

$$\begin{aligned} (y^2 \cdot v_1^{b_1} \cdot v_2^{b_2} \cdot \dots \cdot v_m^{b_m}) \bmod n &= ((z \cdot s_1^{b_1} \cdot s_2^{b_2} \cdot \dots \cdot s_m^{b_m})^2 \cdot v_1^{b_1} \cdot v_2^{b_2} \cdot \dots \cdot v_m^{b_m}) = \\ &= z^2 \cdot (s_1^2 v_1)^{b_1} \cdot (s_2^2 v_2)^{b_2} \cdot \dots \cdot (s_m^2 v_m)^{b_m} \bmod n = z^2 \cdot 1^{b_1} \cdot 1^{b_2} \cdot \dots \cdot 1^{b_m} \bmod n = \\ &= z^2 \bmod n = x. \end{aligned}$$

Shu tarzda t marta iteratsiya bajariladi. Bunday takrorlashlarda har doim z tasodifiy soni qaytadan tanlanadi. Barcha iteratsiyalarning natijalari ijobiy bo'lsa, V tekshiruvchi haqiqatdan ham P abonent s sirni bilishini isbotini qabul qiladi.

Isbot qiluvchi P abonent V tekshiruvchini t marta aldash ehtimoli bu protokolda $1/2^{mt}$ ga teng. Shu bois, protokol mualliflari protokolda $m=5$ va $t=4$ qiymatlardan foydalanishni tavsiya qilishadi.

Misol. Ushbu misolda hisoblashlarni soddalashtirish maqsadida, protokolga zid holda kichik tub sonlaridan foydalaniladi.

T ishonchli markaz $n=5 \cdot 7=35$ modulni hisoblaydi va uni barcha isbotlovchilarga e'lon qiladi. Faraz qilyaylik, isbot qiluvchi P abonent maxfiy kalit vektorini $S=[3,4,9,8]$ ko'rinishda tanladi. U holda P abonent

$$v_i = (s_i^2)^{-1} \bmod n, \quad (i = \overline{1,4})$$

shartdan ochiq kailit $v=[4,11,16,29]$ vektorini hisobladi.

Protokol quyidagicha amalga oshiriladi:

1. P abonent $(1,35)$ oraliqdan tasodifiy $z=16$ sonini tanlaydi va V tekshiruvchiga $x=z^2 \bmod n=16^2 \bmod 35=11$ sonini jo'natadi.

2. V tekshiruvchi $B=[1,1,0,1]$ bitlar vektorini tasodifiy tanlaydi va uni P abonentga jo'natadi.

3. P isbot qiluvchi abonent $y=(16 \cdot 3^1 \cdot 4^1 \cdot 9^0 \cdot 8^1) = 1536 \bmod 35 = 31$ sonini hisoblab, uni V tekshiruvchiga jo'natadi.

1. Alisa va Bob C_1 va C_2 tasodifiy sonlarini birgalikda hosil qilishadi.

2. Alisa $t \cdot k = 1 \pmod{\varphi(n)}$ munosabatdan foydalanib, bir martalik ochiq t va yopiq k kalitlarni shakllantiradi. Bu kalitlarni u har xil shifrlash kalitlaridan foydalanib (t va k kalitlardan birortasi oshkor bo'lib qolsa, ikkinchisi aniqlanmasligi uchun), shifrlaydi. Bu shifrlatmalarni turli tashuvchilarda saqlaydi. Undan so'ng u $C_1^k \pmod n = X_1$ va $C_2^t \pmod n = X_2$ sonlarni hisoblaydi.

3. Alisa (C_1, X_1) va (C_2, X_2) sonlar juftligini Bobga taqdim qiladi. Bob esa r tasodifiy bitni tanlaydi va uni Alisaga taqdim qiladi.

4. Agar $r = 0$ bo'lsa, Alisa k ning qiymatini, agar $r = 1$ bo'lsa t ning qiymatini Bobga taqdim qiladi.

5. Agar $r = 0$ bo'lsa, Bob $C_1^k \pmod n = X_1$ va $X_2^k \pmod n = C_2$ munosabatlarni bajarilishini tekshirib ko'radi. Agar $r = 1$ bo'lsa, Bob $X_1^t \pmod n = C_1$ va $C_2^t \pmod n = X_2$ munosabatlarni bajarilishini tekshirib ko'radi.

Agar ko'rsatilgan munosabatlar o'rinli bo'lsa, Alisa n sonini ko'paytuvchi-larga yoyishni bilishini isbotini Bob qabul qiladi.

Ushbu protokolni biror sirni bilishni masofadan turib, isbotlashga qo'llash mumkin. Bu holda tasodifiy sonlar telefon orqali ikki tomonning ishtirokida birgalikda hosil qilinadi. Bu protokolning yutug'i shundaki, bunda tekshirish uchun ko'p sondagi raundlar talab etilmaydi. Bu esa protokolni amaliyotga qo'llashni soddalashtiradi.

$s = (m')^d \pmod n$ imzoni t^{-1} ga ko'paytirib, C kriptogrammadagi M axborotni tiklash mumkin:

$$s \cdot t^{-1} = (m')^d \cdot t^{-1} = (C \cdot t^e)^d t^{-1} = C^d t^{e \cdot d} t^{-1} = C^d = M \pmod n.$$

Quyida keltirilgan protokoldan foydalanilsa, Bob shubhaga borishiga va Alisa xavotirga tushishiga o'rin qolmaydi.

Protokolda amalga oshiriladigan qadamlar:

1. Alisa va Bob tanga tashlash protokolidan foydalanib, tasodifiy R sonini birgalikda hosil qilishadi.

2. Alisa birgalikda hosil qilingan tasodifiy R sonini imzolaydi:
 $s = R^d \pmod n.$

3. Bob imzoni tekshirib ko'radi: $s^e \pmod n = R.$

Bu protokolni amalga oshirish natijasida Alisa Mellorining yopiq kaliti d ni bilishiga Bobda shubha qolmaydi. Chunki, tasodifiy R sonini hosil qilishda Bobning o'zi bevosita ishtirok etdi. Ammo, Mellorini yopiq kaliti oshkor bo'lganiga Bob uni shontirishi mumkin. Shu sababli bu variant Alisaga ma'qul bolmasligi mumkin. Ammo, Bobning bu harakati unchalik ishonchli emas. Chunki, Bob o'z niyatini amalga oshirishda R soniga mos keluvchi imzoni Melloriga ko'rsatadi. Bu imzoga mos keluvchi xabar (aniqrog'i R soni) ni Bob Mellorining ochiq kaliti e dan foydalanib, $s^e \pmod n = R$ tarzda tiklaydi. Bunda Mellorining yopiq kaliti d ishlatilmadi. Shu sababli Mellori bu holatga ahamiyatsiz deb qaraydi.

§4.10. Bir raundli tekshirishga asoslangan protokol

Ayrim hollarda protokolda bajariladigan hisoblashlarni aloqa kanali bo'yicha himoyalashni imkoni bo'lmagan hollarda bir raundli tekshirishga asoslangan protokoldan foydalanish mumkin. Bunda bir necha bosqichdan iborat tayyorgarlik ishlari amalga oshirilgandan so'ng, isbot qiluvchi abonent bir raundli tekshirishga asoslangan protokolda qandaydir siri bilishini nol oshkoralik bilan isbotlashi mumkin. Quyidagi protokolda isbot qiluvchi abonent vazifasini Alisa bajaradi, tekshiruvchi sifatida Bob ishtirok etadi.

Manuel Blyum tomonidan bir-biridan uzoq masofada bo'lgan ishtirokchilar o'rtasida tanga tashlash yo'li bilan qur'a tashlash masalasini ijobiy hal qilish mumkinligi ko'rsatilgan.

1982 yildagi 24-kompyuter konferensiyasida M.Blyum «Telefon orqali qur'a tashlash: yechilmaydigan muammolarni yechish» mavzusida ma'ruza qildi. Blyum o'z ma'ruzasida ajrashishga qaror qilgan er-xotinlar o'rtasidagi oilaviy mashinani kimga qolishini hal qilish masalasida birinchi marta elektron qur'a tushunchasini kiritdi. U telefondan foydalanib (chunki, er-xotinlar turli shaharlarda yashaydi), tanga tashlash orqali qur'a tashlash yo'li bilan bu oilaviy muammoni oqilona yechish mumkinligini ko'rsatib berdi.

Tanga tashlash protokollari qiyudagi 2 ta talab asosida yaratilgan:

1. Natijani bashorat qiluvchidan eshitgandan so'ng, tanga tashlovchi qaytadan tanga tashlash imkoniga ega bo'masligi lozim;

2. Natijani bashorat qiluvchi o'zining bashoratini e'lon qilmasdan oldin, tanga tashlash natijasini bilish imkoniga ega bo'masligi lozim.

Bu shartlarni protokollarda bajarilishini quyida keltiriladigan real hodisaga qiyoslash mumkin.

Alisa va Bob protokolda ishtirok etuvch shaxslar bo'lsin. Alisa suvi tinq bo'lgan quduq yonida turibdi. Bob esa Alisadan va quduqdan ancha narida turibdi. Ammo, Bob Alisa va uni hatti-harakatini bemalol ko'rish imkoniga ega. Alisa tangani quduqqa tashlaydi. Bob esa tangani qaysi tomon bilan tushganini ko'rish imkoniyatiga ega emas, shu sababli u natijani bashorat qilishda tavakkal qilishga majbur. Quduq yonida turgan Alisa uning tubidagi tangani ko'rish imkoniga ega, lekin natijani o'zgartirolmaydi. Shu sababli kim yutgan yoki yutqazganligini aniqlash uchun Alisa Bobni quduq yoniga chaqirishga majbur.

§5.2. Blyum – Mikal protokoli

A va B ishtirokchilar protokolda foydalanish uchun bir tomonlama f ($f: X \rightarrow Y$) funksiya haqida kelishib olishadi. Bu erda X – teng sondagi juft va toq sonlardan iborat bo'lgan chekli sondagi natural sonlar to'plami. A ishtirokchi – tanga tashlovchi, B ishtirokchi – natijani bashorat qiluvchi.

Protokolda quyidagi qadamlar amalga oshiriladi:

1. $A \rightarrow B: y = f(x)$, bu yerda $x \in X$ – tasodifiy son.

5-BOB. TANGA TASHLASH PROTOKOLLARI

Ma'lumki, kundalik hayotda insonlar o'rtasida turli xil bahs va munozaralarga asoslangan muammolar paydo bo'ladi. Ayrim hollarda bu muammolarni tanga tashlash orqali qur'a tashlash yo'li bilan oson hal qilish mumkin.

Tanga tashlash protokollari hozirgi kunda primitiv protokoli sifatida amaliyotga muvaffaqiyatli qo'llanilmoqda. Ushbu protokollarni amaliyotga qo'llanish sohalari keng. Masalan, futbol, voleybol va basketbol bo'yicha jahon yoki mintaqaviy chempionatlarni (shunga o'xshash tadbirlarni) o'tkazishni tashkillashtirishda komandalarni vakillari dunyoning biror shahriga to'planishib, komandalarni guruhlarga taqsimlash uchun qur'a o'tkazadilar. Bunda katta miqdordagi moliyaviy mablag'lar va tadbir ishtirokchilarining vaqtlari sarf bo'ladi. Bu turdagi tadbirlarni minimal miqdordagi moliyaviy mablag'lar hisobidan juda tez tashkillashtirish mumkin. Bunung uchun kriptografik protokollardan foydalanib, Internet orqali elektron qur'a tashlashni qo'llashni o'zi yetarli. Xuddi shu tarzda halol yo'l bilan loteriya o'yinlarini o'tkazish hamda moliyaviy imkoniyati cheklangan tashkilot xodimlari o'rtasida dam olish maskanlariga imtiyozli yo'llanmalarni ham tarqatish mumkin.

Ushbu bobda tanga tashlashning bir necha protokollari bayon qilinadi. Ushbu protokollarni n marta qo'llab, protokol ishtirokchilari n bitli tasodifiy kalitga ega bo'lishlari mumkin.

§5.1. Tanga tashlash sxemalari

Qur'ada ishtirok etuvchi shaxslar bir joyda, yonma-yon turgan bo'lsalar, bu muammoni odatdagi qur'a tashlash, ya'ni tanga tashlash yo'li bilan ijobiy hal qilish mumkin.

Agar qur'ada ishtirok etuvchi shaxslar turli xil joyda, ya'ni bir-biridan uzoq masofada bo'lsalar, bir qarashda qur'a tashlash masalasi bu holda amalga oshmaydigan masalaga o'xshaydi. Chunki, odatdagi tanga tashlash jarayoniga ko'ra bir ishtirokchi tanga tashlash natijasini oldindan bashorat qiladi. Ikkinchi ishtirokchi esa tangani tashlaydi va natijani o'ziga ma'qul bo'lgan tarzda birinchi ishtirokchiga e'lon qilishi mumkin.

2. $B \rightarrow A$: B ishtirokchi bu shifrlangan xabarlardan birini (gerb yoki raqam deb hisoblaganini) tanlaydi va uni o'zining ochiq kaliti bilan shifrlaydi – $E_B(E_A(M_i))$, bu yerda $i=1$ yoki $i=2$. Bu shifrmanni A ishtirokchiga jo'natadi.

3. $A \rightarrow B$: $D_A(E_B(E_A(M_i))) = E_B(M_i)$. Bu yerda $i=1$ yoki $i=2$.

4. $B \rightarrow A$: $D_B(E_B(M_i)) = M_i$. Bu yerda $i=1$ yoki $i=2$. B ishtirokchi M_i xabarga asosan o'zining yutgan yoki yutqazganligini aniqlaydi.

5. A: Qabul qilingan M_i xabarni M_1 yoki M_2 bilan solishtirib, o'zining yutgan yoki yutqazganligini aniqlaydi.

Tanga tashlash o'yini tamom bo'lgandan so'ng, ya'ni, protokolning oxirida bir-birlarini halol o'ynaganlariga ishonch hosil qilish maqsadida ishtirokchilar o'zlarining ochiq va maxfiy kalitlar juftliklarini bir-birlariga taqdim qiladilar.

§5.5. Shnorr kriptotizimi asosidagi tanga tashlash protokoli

Ishonchli markaz quyidagi parametrlarni tanlaydi va barcha abonentlarga e'lon qiladi:

p, q – katta tub sonlari. p soninig razriyadi 512 bitdan, q soninig razriyadi esa 140 bitdan kam bo'lmasligi tavsiya qilinadi.

$g \in Z_p$ maydon elementi bo'lib, uning tartibi q sonining tartibiga teng (ya'ni, $g^q = 1 \pmod{p}$, $g \neq 1$).

Protokol quyidagi qadamlarni amalga oshirishdan iborat:

1. $A \rightarrow B$: $y = g^x \pmod{p}$. Bu yerda $x \in Z_q$ – tasodifiy son.

2. $B \rightarrow A$: $r = y^b \cdot g^k \pmod{p}$. Bu yerda $b = \{0,1\}$ – tasodifiy bit, $k \in Z_q$ – tasodifiy son.

3. $A \rightarrow B$: α . Bu yerda $\alpha = \{0,1\}$ – tasodifiy bit.

4. $B \rightarrow A$: b, k .

A : $r_1 = y^b \cdot g^k \pmod{p}$ ni hisoblaydi. Agar $r_1 = r$ tenglik o'rinli bo'lsa, A ishtirokchi o'zining yutgan yoki yutqazganini aniqlaydi.

2. $B \rightarrow A: b \in \{0,1\}$. Agar x – joft bo'lsa, $b = 0$. Aks holda $b = 1$.

3. $A \rightarrow B: x$.

B ishtirokchi $f(x) = y$ tenglikni bajarilishini tekshirib, qur'a tashlashda yutgan yoki yutqazganligiga ishonch hosil qiladi.

Protokolni amalga oshirishda shunday masala kelib chiqadi: nega A ishtirokchi x sonni tanlab oldi. Undan ko'ra, qandaydir b bitni tanlab olib, bir tomonlama $y = f(b)$ ni hisoblasa bo'lmasmidi? Gap shundaki, y ni hisoblashda bir tomonlama funksiyaning argumentlar to'plami yetarlicha katta bo'lishi kerak. b bitni 0 va 1 qiymatlar qabul qilishini hisobga olsak, B ishtirokchi osongina $y = f(b)$ qiymatni hisoblab topishi natijasida ulardan qaysi biri y bilan ustma – ust tushushini aniqlay olar edi.

§5.3. Diskret logarifmlashga asoslangan tanga tashlash protokoli

Ushbu protokollar diskret logarifmlash masalasining murakkabligiga asoslangan.

Protokolda ishlatiladigan parametrlar:

p – katta tub son;

$g \in Z_p$ multiplikativ gruppaga tegishli element.

Bu protokol quyidagi qadamlarni amalga oshirishga asoslangan:

1. $A \rightarrow B: y = g^x \text{ mod } p$, bu yerda $x \in Z_p$ – tasodifiy son.

2. $B \rightarrow A: b \in \{0,1\}$. Agar x – juft bo'lsa, $b = 0$. Aks holda $b = 1$.

3. $A \rightarrow B: x$.

$B: g^x \text{ mod } p = x$ tenglikni bajarilishini tekshirib, qur'a tashlashda yutgan yoki yutqazganligiga ishonch hosil qiladi.

§5.4. RSA kriptotizimi asosidagi tanga tashlash protokoli

Ushbu protokolda quyidagi parametrlardan foydalaniladi:

E_A, D_A – mos holda A ishtirokchining ochiq va maxfiy kalitlari;

E_B, D_B – mos holda B ishtirokchining ochiq va maxfiy kalitlari.

Protokolda quyidagi qadamlar amalga oshiriladi:

1. $A \rightarrow B: E_A(M_1), E_A(M_2)$. Bu yerda M_1 va M_2 – A ishtirokchi tomonidan shakllantirilgan xabarlar. Ulardan biri gerbni, ikkinchisi raqamni anglatadi.

6-BOB. SIRNI TAQSIMLASH PROTOKOLLARI

Faraz qilaylik, bir-biri bilan o'zaro do'st bo'lgan 3 kishi katta miqdordagi xazinani o'g'irlashdi. Bu xazinani ular shunday seyfga joylastirishlari kerakki, bu seyfni ularning har biri ochish imkoniga ega bo'lsin. Buning uchun seyfnig kalitini ularning har biriga berish lozim. Bu holda ulardan biri xiyonat yo'lga kirib, boshqalariga bildirmasdan seyfdagi xazinani umarishi mumkin. Seyfdagi xazinani saqlab qolish hamda bir-birlarini aldab ketishlarini oldini olish uchun eng oqilona yo'l – bu ularning har biriga alohida kalit berishdir. Shunda bu do'stlar birgalikda yig'ilib, seyfni ochishlari mumkin bo'ladi.

Sirni taqsimlash protokollari axborot (maxfiy kalit, parol) larni bo'laklab, ulushlarga taqsimlab saqlashga asoslangan. Bu protokollar sir ulushlariga ega bo'lmagan ayrim shaxslar yoki ularning kichik guruhlari sirni tiklash imkoniyatiga ega bo'lmashliklari maqsadida hosil bo'lgan. Ushbu holatda faqatgina sir ulushlariga ega bo'lgan barcha shaxslar yoki ularning katta guruhlari birgalikda yig'ilib, sirni tiklashlari mumkin bo'ladi.

Sirlarni bo'laklab saqlash masalasi ayrim javobgar shaxslar tomonidan jamoa bo'lib yechim qabul qilishga zaruriyat bo'lganda paydo bo'ladi.

§6.1. Sirlarni taqsimlashning asosiy tushunchalari

Sirlarni taqsimlash protokollari – axborotlarni taqsimlab (bo'lak - bo'lak) saqlash uchun ishlatiladi. Ushbu protokolni amalga oshirish natijasida uning ishtirokchilari, ya'ni sirni bilishga haqli bo'lgan shaxslar birgalikda yig'ilib, sirni tiklashlari mumkin. Sirni bilishga haqli bo'lmagan shaxslar guruhi esa hattoki saralash yo'li bilan ham sirni tiklash imkoniga ega bolmasliklari lozim.

Sirlarni taqsimlash protokolida abonent deb nomlanuvchi P_1, P_2, \dots, P_n n ta ishtirokchi hamda sir ulushlarini tarqatuvchi yoki diler deb nomlanuvchi D protokolda ishtirok etadi.

§5.6. Tasodifiy umumiy bitni hosil qilish uchun diskret logarifmlashga asoslangan tanga tashlash protokoli

Tanga tashlash protokollari ko'p hollarda bir – biriga ishonmaydigan abonentlar o'rtasida qandaydir kriptotizimda foydalanish uchun umumiy tasodifiy kalitni hosil qilish uchun qo'llaniladi. Agar abonentlardan biri ikkinchisi unga bardoshli kalit yuborishiga shubhalansa, u holda ushbu shubhalardan xolis bo'lish uchun, tanga tashlashning modifikasiyalashgan protokollaridan foydalanishi mumkin. Ushbu protokollarni n marta qo'llab, abonentlar n bitli tasodifiy kalitga ega bo'lishlari mumkin. Ushbu holatda nafaqat A va B abonentlar, balki g'araz niyatli buzg'unchi ham o'ziga ma'qul bo'lgan o'zgarishlarni ushbu kalitga kiritish imkoniga ega bo'lmaydi.

Ushbu protokol parametrlari:

p – katta tub son;

g – Z_p multiplikativ gruppaga tegishli element.

Bu protokol quyidagi qadamlarni amalga oshirishga asoslangan:

1. $A \rightarrow B$: $y = g^x \pmod p$, bu yerda $x \in Z_p$ – tasodifiy son.

2. $B \rightarrow A$: $r = y^b g^k \pmod p$, bu yerda $b \in \{0,1\}$, $k \in Z_p$ parametrlar tasodifiy tanlanadi.

3. $A \rightarrow B$: tasodifiy $c \in \{0,1\}$.

4. $B \rightarrow A$: b, k .

5. A : $y^b g^k \pmod p = r$ tenglikni tekshirib ko'radi. Bu tekshirish natijasi ijobiy yakunlansa, ushbu protokolning natijasi $d = b \oplus c$ tasodifiy bit bo'ladi.

Shuni qayd qilish lozinki, k parameter Z_p gruppadan tasodifiy tanlanganligi hamda $b=0$ da ham $b=1$ da ham r parameter Z_p^* gruppaning tasodifiy elementi bo'lib qolishi sababli, A ishtirokchi r parameterning qiymatidan b bitning qiymatini aniqlay olmaydi. Ya'ni, k parameterning qiymati noma'lum bo'lgan holda r, g va p parameterlarning qiymatlardan b bitning qiymatini bilish mumkin emas. Protokolda A ishtirokchi y ni Z_p^* gruppaga tegishli bo'lmagan element sifatida tanlab, B ishtirokchini aldashga harakat qilishi mumkin. Lekin, buni $y^b \pmod p = 1$ taqqoslama bilan tekshirib ko'rish mumkin. Shu sababli u B ishtirokchiga tasodifiy c bitni jo'natishga majbur.

Ushbu protokolni abonentlar n marta qo'llab, n bitli tasodifiy bitlar ketma-ketligini hosil qilishlari mumkin.

ruxsat etilgan guruh sifatida abonentlar soni k dan kam bo'lmagan ixtiyoriy guruh qatnashishi mumkin.

Blekli sxemasi. Ma'lumki k noma'lumli tub son moduli bo'yicha hosil qilingan chiziqli erkli k taqqoslamalar yagona yechimga ega bo'ladi. 1979 yilda yaratilgan Blekli sxemasi shunga asoslangan. n ta abonentlar o'rtasida m sir shunday taqsimlanadiki, abonentlar soni k dan kam bo'lmagan ixtiyoriy guruh sirni bilishga ruxsat etilishi mumkin.

Blekli sxemasida quyidagi parametrlardan foydalaniladi:

p - katta tub son. p soni ushbu sxema bo'yicha tarqatiladigan ixtiyoriy sirdan katta bo'lishi kerak ($p > m$). U holda $m \in Z_p$.

n – sir ulushlari soni.

k – sirni bilishga ruxsat etilgan guruhning minimal o'lchovi.

Tayyorgarlik bosqichi.

Tasodifiy ravishda sirni tarqatuvchi $x_2^*, x_3^*, \dots, x_k^* \in Z_p$ sonlarini tanlaydi, ya'ni $Q = (m, x_2^*, x_3^*, \dots, x_k^*)$ sir nuqtasi hosil qilinadi.

Sirni taqsimlash bosqichi.

Sirni taqsimlovchi i ($i=1, \dots, n$) ishtirokchilar uchun Z_p guruhda tasodifiy tekis taqsimlangan $a_{1i}, a_{2i}, \dots, a_{ki}$ sonlarni tanlaydi va $b_i = a_{1i}m + a_{2i}x_2^* + \dots + a_{ki}x_k^* \pmod p$ ni hisoblaydi. Shundan so'ng tarqatuvchi P_i abonentlarga

$$a_{1i}x_1 + a_{2i}x_2 + \dots + a_{ki}x_k \equiv b_i \pmod p$$

taqqoslamalarni x_1, x_2, \dots, x_k noma'lumlari bilan birgalikda $a_{1i}, a_{2i}, \dots, a_{ki}$ koeffitsientlarini jo'natadi. Bunda tarqatuvchi shunga e'tibor berishi lozimki, ixtiyoriy k taqqoslamalar chiziqli erkli bo'lishlari lozim.

Sirni tiklash bosqichi.

Bu bosqichda k abonentlar birgalikda yig'ilib, o'zlaridagi taqqoslamalardan quyidagi taqqoslamalar sistemasini hosil qilishlari mumkin:

$$a_{11}x_1 + a_{21}x_2 + \dots + a_{k1}x_k \equiv b_1 \pmod p$$

$$a_{12}x_1 + a_{22}x_2 + \dots + a_{k2}x_k \equiv b_2 \pmod p$$

.....

$$a_{1k}x_1 + a_{2k}x_2 + \dots + a_{kk}x_k \equiv b_k \pmod p.$$

Barcha abonentlar to'plamini $P = \{P_1, P_2, \dots, P_n\}$ bilan belgilaymiz. Sirni bilishga haqli bo'lgan abonentlar to'plamini A bilan belgilaymiz.

$A \subseteq P$ to'plam sirni bilishga ruxsat etilgan guruh deb nomlanadi.

Sirni bilishga ruxsat etilgan barcha guruhlar to'plami Γ ni ruxsat etilganlar tuzilmasi (strukturasi) deb nomlanadi.

P dagi ixtiyoriy abonent ruxsat etilgan biror–bir guruhda ishtirok etadi deb faraz qilinadi. Aks xolda ularning abonent sifatida P da ishtirok etishi ma'noga ega bo'lmay qoladi.

Shuningdek, Γ to'plamni yopiq deb hisoblaymiz. Ya'ni, agar $A \subseteq B \subseteq P$ va $A \in \Gamma$ bo'lsa, bundan kelib chiqadiki, $B \in \Gamma$. Haqiqatdan ham P_1, P_2, \dots, P_n abonentlar sirni tiklashlari mumkin bo'lsa, agar ular safiga bir necha $P_{k+1}, P_{k+2}, \dots, P_{k+t}$ abonentlar qo'shilsa, hosil bo'lgan yangi guruhni kalitni tiklashi osonlashadi.

Sirni taqsimlash protokollari ikki bosqichdan iborat:

➤ sirni taqsimlash yoki tarqatish;

➤ sirni tiklash.

1. *Sirni taqsimlash yoki tarqatish.*

Bu bosqichda m sirni biluvchi diler sirni m_1, m_2, \dots, m_n sir ulushlarga ajratadi va m_i sir ulushini P_i ($i = \overline{1, n}$) ishtirokchiga himoyalangan kanal orqali uzatadi.

Sirni taqsimlash shunday tashkillashtirilishi kerakki, sirni bilishga haqli bo'lgan abonentlarning guruhlari birgalikda yig'ilib m sirni tiklash imkoniga ega bo'lsin. Sirga ruxsati bo'lmaganlar esa sirni bilish imkoniyatiga ega bo'lmasinlar.

2. *Sirni tiklash bosqichi.*

Bu bosqichda Γ ruxsat etilganlar tuzilmasidagi biror – bir guruh o'zlaridagi m_i ($i = \overline{1, n}$) sir ulushlarini birlashtirib m sirni tiklaydilar.

§6.2. Sirni taqsimlashning bo'sag'ali sxemalari

Sirni taqsimlashning (n, k) ($k \leq n$) bo'sag'ali sxemalari deb shunday sxemaga aytiladiki, bunda sir n ta ishtirokchi o'rtasida bo'linadi va sirga

Ushbu taqqoslamalar sistemasining matrisasi kengaytirilgan ko'rinishga keltiriladi va bu sistema Gauss usulida Z_{11} to'plamda yechiladi:

$$\begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 3 & 2 & 7 & | & 4 \\ 8 & 1 & 10 & | & 8 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & -1 & 4 & | & -20 \\ 0 & -7 & 2 & | & -56 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & 10 & 4 & | & 2 \\ 0 & 4 & 2 & | & 10 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & 1 & 7 & | & 9 \\ 0 & 4 & 2 & | & 10 \end{pmatrix}_{11} \Rightarrow \\ \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & 1 & 7 & | & 9 \\ 0 & 0 & 7 & | & 7 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 0 & | & 7 \\ 0 & 1 & 0 & | & 2 \\ 0 & 0 & 1 & | & 1 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & | & 5 \\ 0 & 1 & 0 & | & 2 \\ 0 & 0 & 1 & | & 1 \end{pmatrix}_{11}.$$

Taqqoslamalar sistemasini yechib, $x_1=5$, $x_2=2$, $x_3=1$ ni topamiz. Birinchi noma'lumning qiymati aynan $m=5$ sirni ifodalaydi.

Faraz qilaylik, P_1 va P_2 abonentlar, P_3 abonent ishtirokisiz sirni tiklashmoqchi bo'lsalar, unda ular sirni tiklay oladilarmi? Bu holda ular shtirokidagi taqqoslamalar sistemasining matrisasi quyidagi kengaytirilgan ko'rinishda bo'ladi:

$$\begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 3 & 2 & 7 & | & 4 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & -1 & 4 & | & -20 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 1 & 1 & | & 8 \\ 0 & 1 & 7 & | & 9 \end{pmatrix}_{11} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & | & 10 \\ 0 & 1 & 7 & | & 9 \end{pmatrix}_{11}$$

Bu taqqoslamalar sistemasining yechimi

$$m=x_1=10-x_3 \text{ mod } 11,$$

$$x_2=9-7x_3 \text{ mod } 11.$$

Bu holda m - sir 0 va 10 oralig'dagi ixtiyoriy qiymatni qabul qilishi mumkin. Shunday qilib, P_1 va P_2 abonentlar birgalikda (P_3 abonent ishtirokisiz) sirni tiklay olmadilar.

§6.3. Lagranj interpoliyasion ko'phadiga asoslangan Shamir sxemasi

Shamir sxemasi $k-1$ tartibli interpoliyasion ko'phad qurish uchun k nuqtadan foydalanishga asoslangan. Bu yerda ham Blekli sxemasi parametrlaridan foydalaniladi:

Ushbu taqqoslamalar sistemasini yechib, Q nuqtani topishlari mumkin, ushbu nuqtaning birinchi koordinatasi m sir bo'ladi.

Eslatma:

1) p etarlicha katta tub son bo'lsa, taqqoslamalar koeffisientlarini tasodifiy tanlanishi e'tiborga olinsa, taqqoslamalarni chiziqli erkli bo'lish shartini hisobga olmaslik mumkin, chunki bu shartning buzilish ehtimoli kam.

2) Agar $t < k$ abonentlar birlashib sirni tiklamoqchi bo'lsa, bu sirni tiklashning iloji yo'q, chunki ular tomonidan tuzilgan taqqoslamalar sistemasi kerakli yechimni emas, balki k o'lchovli fazodagi t - tartibli gipertekislikda yotuvchi nuqtalar to'plamini beradi. Bu to'plamda qaysi biri sirli nuqta ekanligini topish amalda mumkin emas. Ya'ni, ushbu holda sir sifatida Z_p dan olingan ixtiyoriy qiymat teng ehtimollik bilan sir bo'lishi mumkin.

Misol. $m=5$ - sir, $p=11$ - modul, $Q=(m=5, x_2^*=2, x_3^*=1)$ - sir nuqtasi bo'lsin.

Sirni taqsimlash bosqichi.

Abonentlar uchun Z_p guruhda tasodifiy tekis taqsimlangan $a_{1i}, a_{2i}, \dots, a_{ki}$ sonlari tanlanadi. Bu sonlar va sir nuqtasi koordinatalari asosida b_i ($i = \overline{1,3}$) soni (bu son va $a_{1i}, a_{2i}, \dots, a_{ki}$ sonlari birgalikda i abonentning sur ulushini tashkil qiladi) quyidagicha hisoblanadi:

P_1 uchun: $a_{11}=1, a_{21}=1, a_{31}=1$. U holda $b_1=1 \cdot 5 + 1 \cdot 2 + 1 \cdot 1 \pmod{11} = 8$.

P_2 uchun: $a_{12}=3, a_{22}=2, a_{32}=7$. U holda $b_2=3 \cdot 5 + 2 \cdot 2 + 7 \cdot 1 \pmod{11} = 4$.

P_3 uchun: $a_{13}=8, a_{23}=1, a_{33}=10$. U holda $b_3=8 \cdot 5 + 1 \cdot 2 + 10 \cdot 1 \pmod{11} = 8$.

Sirni tiklash bosqichi.

Bu bosqichda abonentlar taqqoslamalaridan quyidagi taqqoslamalar sistemasini hosil qilish mumkin:

$$\begin{cases} x_1 + x_2 + x_3 \equiv 8 \pmod{11} \\ 3x_1 + 2x_2 + 7x_3 \equiv 4 \pmod{11} \\ 8x_1 + x_2 + 10x_3 \equiv 8 \pmod{11} \end{cases}$$

Abonentlarning sir ulushlarini birlashtirib, Lagranj interpolyasion ko'phadini quyidagicha qurish mumkin:

$$\begin{aligned}
 S(x) &= 6 \frac{(x-2)(x-3)}{(1-2)(1-3)} + 6 \frac{(x-1)(x-3)}{(2-1)(2-3)} + 18 \frac{(x-1)(x-2)}{(3-1)(3-2)} \pmod{31} = \\
 &= 3(x^2 - 5x + 6) - 6(x^2 - 4x + 3) + 9(x^2 - 3x + 2) \pmod{31} = 18 - 18x + 6x^2 \pmod{31} = \\
 &= 18 + 13x + 6x^2 \pmod{31}.
 \end{aligned}$$

Bundan ko'rinadiki, $m=S(0)=18$. Demak, sir tiklandi.

§6.4. Qoldiq haqidagi Xitoy teoremasiga asoslangan sirni taqsimlash sxemasi

Sirni taqsimlashining bo'sag'ali sxemasini qurishga zamin bo'ladigan teoremani keltiramiz.

Qoldiq haqidagi Xitoy teoremasi.

m_1, \dots, m_k – jufti-jufti bilan tub sonlar bo'lsa, u holda

$$\begin{cases}
 x \equiv b_1 \pmod{m_1} \\
 x \equiv b_2 \pmod{m_2} \\
 \dots \dots \dots \\
 x \equiv b_k \pmod{m_k}
 \end{cases}$$

taqqoslamalar sistemasi quyidagi yagona yechimga ega

$$x_0 \equiv \sum_{i=1}^k b_i M_i M'_i \pmod{M},$$

bu yerda $M = \prod_{i=1}^k m_i = EKK(m_i)$, $M_i = \frac{M}{m_i}$, $M'_i = M_i^{-1} \pmod{m_i}$.

Qoldiq haqidagi Xitoy teoremasiga asoslangan sirni taqsimlash sxemasi quyidagi tarzda quriladi.

N-umumiy sir bo'lsin.

Sirni taqsimlash bosqichi.

p_1, p_2, \dots, p_n – turli tub sonlari tanlanadi. U holda i abonentga mos keluvchi sirning qiymati $x_i \equiv N \pmod{p_i}$. Bunda p_1, p_2, \dots, p_n tub sonlari

p - katta tub son. p soni ushbu sxema bo'yicha tarqatiladigan ixtiyoriy sirdan katta bo'lishi kerak ($p > m$). U holda $m \in \mathbb{Z}_p$.

n - sir ulushlari soni.

k - sirni bilishga ruxsat etilgan guruhning minimal o'lchovi.

Tayyorgarlik bosqichi:

Diler \mathbb{Z}_p to'plamdan s_1, s_2, \dots, s_{k-1} sonlarni tasodifiy tanlaydi, ulardan foydalanib

$$S(x) = m + s_1x + s_2x^2 + \dots + s_{k-1}x^{k-1} \pmod{p}$$

maxfiy polinomni quradi.

Taqsimlash bosqichi:

Diler guruhdagi har bir i abonentga tegishli sir ulushlari $(i, S(i))$ ni jo'natadi.

Sirni tiklash bosqichi:

Sirni bilishga haqli bo'lgan i_1, i_2, \dots, i_k nomerli k ta ishtirokchi o'zlarining sir ulushlarini birlashtiradilar: $(i_1, S(i_1)), (i_2, S(i_2)), \dots, (i_k, S(i_k))$. Ular asosida $k-1$ tartibli Lagranj interpoliyasion ko'phadi quyidagicha quriladi:

$$S(x) = \sum_{j=1}^k S(x_j) \frac{(x-x_1) \cdot \dots \cdot (x-x_{j-1}) \cdot (x-x_{j+1}) \cdot \dots \cdot (x-x_k)}{(x_j-x_1) \cdot \dots \cdot (x_j-x_{j-1}) \cdot (x_j-x_{j+1}) \cdot \dots \cdot (x_j-x_k)}$$

Sir $m = S(0)$ sifatida aniqlanadi.

Misol. $m = 18$ - sir, $p = 31$ - modul bo'lsin.

Tayyorgarlik bosqichi:

Diler $s_1 = 13, s_2 = 6$ koeffitsientlarni tanlaydi. U holda maxfiy polinom

$$S(x) = 18 + 13x + 6x^2$$

ko'rinishda bo'ladi.

Sirni taqsimlash bosqichi.

Abonentlarni ulushlarini tashkil etuvchilari quyidagicha bo'ladi:

$$P_1: S(1) = 18 + 13 \cdot 1 + 6 \cdot 1 \pmod{31} = 37 \pmod{31} = 6;$$

$$P_2: S(2) = 18 + 13 \cdot 2 + 6 \cdot 4 \pmod{31} = 68 \pmod{31} = 6;$$

$$P_3: S(3) = 18 + 13 \cdot 3 + 6 \cdot 9 \pmod{31} = 111 \pmod{31} = 18.$$

Sirni tiklash bosqichi:

Sir tiklandi.

Faraz qilaylik, P_1 va P_2 abonentlar, P_3 abonent ishtirokisiz simi tiklashmoqchi bo'lsalar, unda ular sirni tiklay oladilarmi? Bu holda ular o'zlaridagi taqqoslamalardan quyidagi taqqoslamalar sistemasini hosil qiladilar:

$$\begin{cases} N \equiv 10 \pmod{11} \\ N \equiv 3 \pmod{13} \end{cases}$$

Bundan $N = 10 \cdot 13 \cdot 6 + 3 \cdot 11 \cdot 6 \pmod{11 \cdot 13} = 780 + 198 \pmod{143} = 978 \pmod{143} = 120$ ni hosil qiladilar. Ko'rinib turibdiki, ular sirni tiklay olmadilar.

§6.5. Ixtiyoriy tuzilmaga ega bo'lgan guruhlar o'rtasida sirni taqsimlash

6.1 paragrafda ruxsat etilganlar tuzilmasi (strukturasi) Γ sirni bilishga ruxsat etilgan barcha guruhlar to'plami sifatida ta'riflangan edi. Ushbu paragrafda ixtiyoriy tuzilmaga ega bo'lgan guruhlar o'rtasida sirni taqsimlash masalasi o'rganiladi.

(n, n) – bo'sag'ali sxema.

Faraz qilaylik, n ta ishtirokchi o'rtasida taqsimlanadigan sir m bo'lsin. Ruxsat etilganlar tuzilmasi (strukturasi) Γ faqatgina bitta to'plam P dan iborat bo'lsin, ya'ni $\Gamma = \{P\} = \{P_1, P_2, \dots, P_n\}$. Modul d $d > m$ shart asosida tanlanadi.

Sirlarni taqsimlash bosqichi.

Z_d guruhdan s_1, s_2, \dots, s_{n-1} tasodifiy sonlar tanlanadi va

$$s_n = m - s_1 - s_2 - \dots - s_{n-1} \pmod{d}$$

soni hisoblanadi. s_1, s_2, \dots, s_{n-1} sonlar tasodifiy bo'lganligi bois, s_n ham tasodifiy bo'ladi. Ushbu s_i sonlari sirni ulushi sifatida diler tomonidan P_i ishtirokchilarga jo'natiladi.

Sirlarni tiklash bosqichi.

P_1, P_2, \dots, P_n ishtirokchilar o'zlaridagi s_i sirlarni birlashtirib, sirni quyidagi tarzda tiklaydilar:

$$m = s_1 + s_2 + \dots + s_n \pmod{d}.$$

shunday tanlanishi kerakki, ularning ixtiyoriy k tasini ko'paytmasi N dan katta bo'lishi kerak. Bu shart faqat $p_i > \sqrt[k]{N}$ da bajariladi.

$k-1$ ta abonent birgalikda k -chi abonent ishtirokisiz sirni tiklash imkonini mavjud bo'lmashligi uchun $p_i \ll \sqrt[k]{N}$ bo'lishi kerak. Demak, $\sqrt[k]{N} < p_i \ll \sqrt[k]{N}$ $i \in \{1, \dots, n\}$ shart bajarilishi kerak.

Sirni tiklash bosqichi.

Bu bosqichda k ta abonent birgalikda yig'ilib, o'zlaridagi taqqoslamalardan quyidagi taqqoslamalar sistemasini hosil qilishlari mumkin:

$$\begin{cases} N \equiv x_1 \pmod{p_1} \\ N \equiv x_2 \pmod{p_2} \\ \dots \\ N \equiv x_k \pmod{p_k} \end{cases}$$

Taqqoslamalar sistemasini yechilib, N sir aniqlanadi.

1-misol. Sir $N=549$ bo'lsin. Tub sonlar tanlanadigan oraliqlar aniqlanadi:

$$\sqrt[3]{N} \approx 8,2, \sqrt[2]{N} \approx 23,4. \text{ Demak, } 8,2 < p_i \ll 23,4.$$

U holda, $p_1=11, p_2=13, p_3=17$ deb tanlash mumkin.

Sirni taqsimlash bosqichi:

$$x_1 = N \bmod p_1 = 549 \bmod 11 = 10;$$

$$x_2 = N \bmod p_2 = 549 \bmod 13 = 3;$$

$$x_3 = N \bmod p_3 = 549 \bmod 17 = 5.$$

$$P_1 \text{ ni ulushi: } (x_1=10, p_1=11);$$

$$P_2 \text{ ni ulushi: } (x_2=3, p_2=13);$$

$$P_3 \text{ ni ulushi: } (x_3=5, p_3=17).$$

Sirni tiklash bosqichi:

P_1, P_2 va P_3 abonentlar quyidagi taqqoslamalar sistemasini tuzishadi va qoldiq haqidagi Xitoy teoremasi asosan bu sistemani yechishadi:

$$\begin{aligned} N &= 10 \cdot 221 \cdot 1 + 3 \cdot 187 \cdot 8 + 5 \cdot 143 \cdot 5 \bmod 11 \cdot 13 \cdot 17 = 2210 + 4488 + 3575 \bmod \\ &2431 = 2210 + 2057 + 1144 \bmod 2431 = 549. \end{aligned}$$

biriga nisbatan o'zaro ishonchga ega bo'lgan ishtirokchilar sifatida qaralgan edi.

Endi protokolda ishtirok etuvchilarning ayrimlari bir biriga nisbatan raqib bo'lishi mumkin holatda sirni bo'lishish masalasini ko'rib chiqamiz.

Agar diler firibgar bo'lsa ushbu holda protokolda ishtirok etuvchi halol ishtirokchilar sirni taqsimlashni boshqa bir halol dilerga topshirib vaziyatdan chiqishlari mumkin.

Sirni taqsimlashni tekshirish mumkin bo'lgan sxemasi g'oyasi protokolda ishtirok etuvchi g'araz niyatli ishtirokchilarning ayyorona harakatidan halol ishtirokchilarni himoyalashdir. Ushbu g'oya quyidagilardan iborat.

Sirni taqsimlash bosqichida diler sirni shifrlab, e'lon qiladi. Bunda hech kim sirni o'zicha tiklolmaydi. Ammo, taqsimlangan sirni tekshirish sxemasi asosida har bir abonent yoki ishtirokchi sirning o'zidagi ulushidan foydalanib, haqiqatdan ham ushbu ulush sirdan olinganligini tekshirib ko'rishlari mumkin.

Agar ishtirokchilardan ayrimlari buzg'unchi bo'lsalar, u holda bu g'irrom ishtirokchilar o'zlaridagi sirni ulushlarini o'rniga boshqa qiymatlarni jo'natib, sirni tiklashga halaqit qilishlari mumkin. Protokoldan esa umumiy soni t dan kam bo'lmagan halol ishtirokchilar hamma vaqt m sirning qiymatini to'g'ri tiklashlari talab etiladi.

Diskret logarifmlashga asoslangan Shamir sxemasini ko'rib chiqamiz. Bu sxemada sir ulushlarini tarqatuvchi diler koefitsientlari tasodifiy bo'lgan

$$S(x) = s_0 + s_1x + \dots + s_{t-1}x^{t-1}$$

ko'hadni quradi. Bu yerda s_0 -sir. Bu ko'hadga tegishli bo'lgan $S(j)$ nuqtalarni sirni ulushi sifatida diler ishtirokchilarga tarqatadi.

Diler tomonidan firibgarlarni yo'qotish maqsadida, sir ulushlarini tarqatish bosqichidan oldin diler

$$r_i = g^{s_i} \bmod p, \quad i = \overline{0, t-1},$$

hisoblashlarni amalga oshirishi talab etiladi. Bu yerda $g - Z_p^*$ multiplikativ gruppasi elementi. Bu hisoblashlardan so'ng diler r_i ($i = \overline{0, t-1}$)

Misol. Sir $m=120$ bo'lsin. U holda modul d ni $d=143$ deb tanlash mumkin.

Sirni taqsimlash bosqichi.

Z_d guruhdan $s_1=132, s_2=140$ tasodifiy sonlar tanlanadi.

$$\begin{aligned} s_3 &= m - s_1 - s_2 \bmod d = 120 - 132 - 140 \bmod 143 = -152 \bmod 143 = \\ &= -9 \bmod 143 = 134 \bmod 143 = 134. \end{aligned}$$

soni hisolanadi. Bu s_1, s_2 va s_3 , sonlari diler tomonidan mos holda P_1, P_2 va P_3 ishtirokchilarga jo'natiladi.

Sirni tiklash bosqichi.

P_1, P_2 va P_3 ishtirokchilar o'zlaridagi s_i ($i=1,2,3$) sirlarni birlashtirib, sirni quyidagi tarzda tiklaydilar:

$$m = 132 + 140 + 134 \bmod 143 = 406 \bmod 143 = 120 \bmod 143 = 120.$$

Ixtiyoriy tuzilmaga ega bo'lgan guruhlar o'rtasida sirlarni taqsimlash sxemasi quyida keltirilgan tarzda quriladi.

Faraz qilaylik, ruxsat etilganlar tuzilmasi Γ sirni bilishga haqli bo'lgan ishtirokchilarning t ta turli guruhlari to'plamidan iborat bo'lsin, ya'ni $\Gamma = \{A_1, A_2, \dots, A_t\}$, bu yerda $A_i \subseteq P$ ($i=1, \dots, t$) hamda bu A_i to'plamlar har birining quvvati $|A_i| = r_i$ ($i=1, \dots, t$) bo'lsin. U holda A_i to'plamlarning har biri uchun yuqorida bayon etilgan $(n, n) -$ bo'sag'ali sxemani qo'llash mumkin. Agar P_j ($j=1, 2, \dots, n$) ishtirokchi bir vaqtning o'zida sirni bilishga ruxsat etilgan turli guruhlarining a'zosi bo'lsa, u holda ushbu ishtirokchi bu guruhlardan turli sir ulushlarini qabul qiladi. Konkret ishtirokchidagi sir ulushlari guruhning tartib raqami bilan qayd qilinadi.

Aytaylik, sirni bilishga ruxsat etilgan A_i guruh sirni tiklashni istab qoldi. U holda bu guruh a'zosi bo'lgan barcha ishtirokchilar o'zlaridagi i -chi sir ulushlarini sirni tiklash uchun birlashtirishlari lozim bo'ladi.

§6.6. Taqsimlangan sirni tekshirish sxemasi

Oldingi o'tilgan mavzularda sirni taqsimlash sxemalarida sirni tarqatish bosqichida diler ishonchli, sirni tiklash bosqichida esa ishtirokchilar (sirni bilishga haqli odamlar) bir biriga raqib bo'lmagan, bir-

$$r_0 = 19^{10} \bmod 23 = 6,$$

$$r_1 = 19^{13} \bmod 23 = 7,$$

$$r_2 = 19^{20} \bmod 23 = 13.$$

Bu hisoblashlardan so'ng diler r_i ($i = \overline{0,2}$) parametrlarni e'lon qiladi.

Sir ulushlarini taqsimlash bosqichi. Diler sir ulushlarini oldingi bosqichda qurilgan ko'phaddan foydalanib, hisoblaydi:

$$S(1) = 10 + 13 \cdot 1 + 20 \cdot 1^2 = 43,$$

$$S(2) = 10 + 13 \cdot 2 + 20 \cdot 2^2 = 116,$$

$$S(3) = 10 + 13 \cdot 3 + 20 \cdot 3^2 = 229.$$

Diler P_j $j = \overline{1,3}$ ishtirokchilarga tegishli ushbu $S(j)$ sir ulushini jo'natadi.

Taqsimlangan sir ulushlarini tekshirish bosqichi.

Masalan, P_1 ishtirokchi sirni ulushlarini tekshirish uchun qolgan P_2 va P_3 ishtirokchilarga o'zlaridagi sir ulushlarini jo'natishlarini so'rab, so'rovnoma jo'natadi. Sir ulushlarini qabul qilgan P_1 ishtirokchi (*) taqqoslamadan foydalanib,

$$19^{S(1)} \equiv r_0 r_1^1 r_2^{1^2} \pmod{23}$$

hisoblashlarni bajaradi. Unga tegishli $S(1)$ miqdor haqiqatan ham sir ulushi ekanligini tekshirib ko'radi:

$$19^{43} \equiv 6 \cdot 7^1 \cdot 13^{1^2} \pmod{23},$$

$$19^{43} \equiv 6 \cdot 7 \cdot 13 \pmod{23}.$$

P_1 ishtirokchi $17 \equiv 17 \pmod{23}$ natijaga ega bo'ladi. Demak, g'irromlik yo'q.

parametrlarni e'lon qiladi va P_j ishtirokchiga unga tegishli $S(j)$ sir ulushini jo'natadi. Bu sir ulushini qabul qilgan P_j ishtirokchi

$$g^{S(j)} \equiv r_0 r_1^j \dots r_{t-1}^{j^{t-1}} \pmod{p} \quad *$$

taqqoslamani tekshirib, unga tegishli $S(j)$ miqdor sir ulushi ekanligiga ishonch hosil qiladi. Haqiqatan ham

$$r_0 r_1^j \dots r_{t-1}^{j^{t-1}} \equiv g^{s_0} g^{s_1 j} \dots g^{s_{t-1} j^{t-1}} \equiv g^{s_0 + s_1 j + \dots + s_{t-1} j^{t-1}} \equiv g^{S(j)} \pmod{p}$$

taqqoslama o'rinni.

Boshqa tomondan e'lon qilingan r_i ($i = \overline{0, t-1}$) prametrlardan g'irrom ishtirokchilar s_i ($i = \overline{0, t-1}$) koeffisientlar qiymatlarini hisoblashlarini imkoni yo'q. Bu hisoblashlar diskret logarifmlashga asoslanganligi sababli yetarlicha katta p tub sonlari uchun ular murakkab hisoblanadi. Hozirgi kunda ularni hisoblashni samarali yo'llari mavjud emas.

G'irrom ishtirokchilarning firibgarligidan qutilish uchun quyidagi tarzda ishlash lozim bo'ladi.

P_i (abonent) - sirni tiklashni xohlovchi halol abonent bo'lsin u boshqa abonentlarga sirni tiklash uchun so'rovnomaga jo'natadi. Ushbu abonentlarning har biri P_i abonentga o'zlaridagi $S(j)$ ($j \neq i$) ulushlarini jo'natadi. Bu ulushlarni olganidan so'ng, P_i abonent (*) taqqoslama bajarilishini tekshirib ko'radi. Bu tekshiruvdan o'tmagan sir ulushlari usbu protokoldan chiqarib tashlanadi. Agar halol abonentlar soni t dan kam bo'lmasa, P_i (abonent) ushu bobning oldingi mavzularida keltirilgan sirni tiklash bosqichlaridan foydalanib, sirni tiklashi mumkin.

1-misol. Diler ko'hadni koeffisientlarini tasodifiy ravishda quyidagicha tanlaydi:

$$s_0=10, s_1=13, s_2=20.$$

U holda ko'had

$$S(x)=10+13x+20x^2$$

ko'rinishda bo'ladi. Bu yerda $s_0=10$ - sir. Z_p^* multiplikativ gruppaga elementini $g=19$ va modulni $p=23$ tarzda tanlash mumkin. Endi diler $r_i = g^{s_i} \pmod{p}$, $i = \overline{0, 2}$ parametrlar qiymatlarini hisoblaydi:

tekshiruvchi kompyuterdan foydalanilsa, zarur bo'lgan kalitni aniqlash uchun o'rtacha 2285 yil kerak bo'ladi.

Shuningdek, agar kalit uzunligi 64 bit bo'lsa, u holda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^{64} ta kalitni ichidan zarur bo'lgan kalitni aniqlash uchun superkompyuterga 585000 yilga yaqin vaqt kerak bo'ladi.

Ko'rinib turibdiki, kalitlarni aniqlashda hisoblashlarda zarur bo'ladigan hisoblash texnikasi resurslari, aniqrog'i, ularga sarf bo'ladigan xarajatlar ham muhim o'rin egallaydi.

Agar buzg'unchi kalitni sindirishni juda xohlasa, u holda u mablag' sarflashiga to'g'ri keladi. Shu bois, kalitni "minimal" bahosini aniqlash lozim bo'ladi: kalitni ochish iqtisodiy manfaatli bo'lishi uchun kalitni ochishda qanday narx atrofidagi xarajatlardan foydalanishni bilish kerak bo'ladi. Bundan tashqari ko'pgina xabarlarining narxi vaqt o'tishi bilan tez arzonlashadi.

Faraz qilaylik, shifrlangan ma'lumotni qiymati 200\$ bo'lsa, unda narxi 10 million bo'lgan apparaturani o'rnatishni ma'nosi yo'q. Boshqa tomondan ochiq ma'lumotni qiymati 100 million dollar bo'lsa, u holda ushbu xabarning shifrlatishini dastlabki matnga o'girish kalitni aniqlashda foydalanilgan apparaturani narxini qoplaydi.

Hozirgi vaqtda simmetrik kriptotizimlar uchun uzunligi 80 bitdan kam bo'lmagan va asimmetrik kriptotizimlar uchun uzunligi 768 bitdan kam bo'lmagan kalitlarni ishonchli deb hisoblash qabul qilingan. Albatta, bunday baholash shartli baholashdir. Bu yerda asosan kalitlarni bo'lishi mumkin bo'lgan barcha variantlari ichidan zarur bo'lgan kalitni aniqlash imkoniyati hisobga olingan.

Quyidagi jadvalda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari usuliga nisbatan bir xil bardoshlilikka ega bo'lgan simmetrik va asimmetrik kriptotizimlar kalitlarining bitlari uzunligi haqida ma'lumotlar keltirilgan.

7-BOB. SHIFRLASH KALITLARINI GENERASIYA QILISH VA BOSHQARISH

Axborotlarni kriptografik himoyalashda kalitlarga katta e'tibor beriladi. Odatda shifrlash algoritmlari ma'lum deb faraz qilinadi. Demak, shifrni mustahkamligi kalitlarni bardoshligi bilan aniqlanadi. Simmetrik shifrlash tizimlarida va ularga asoslangan protokollarda shifrlashda va dastlabki matnga o'girishda ham kriptobardoshlik kalitning bardoshligiga bog'liq.

Ochiq kalitli kriptotizimlarda shifrlash kalitlari ochiq bo'ladi. Shu sababli ushbu turdagi kriptotizimlarning bardoshligi dastlabki matnga o'girish kalitlarini bardoshligi bilan to'liq xarakterlanadi.

Kalitlarni bosqarish masalasi kalitlarni hayotiyliigi bilan bog'liq bo'lgan quyidagi jarayonlarni to'g'ri amalga oshirish bilan bog'liq:

- kalitlarni generasiya qilish;
- kalitlarni saqlash;
- kalitlarni tarqatish;
- kalitlarni almashtirish;
- kalitlarni yo'q qilib tashlash.

§7.1. Shifrlash kalitlari uzunligi

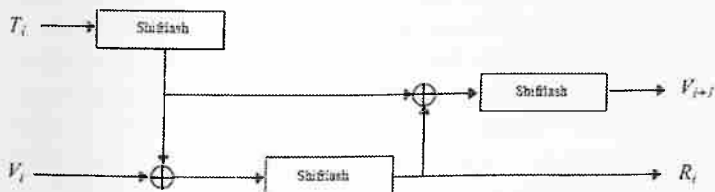
Odatda kalitlarni bardoshligi kalitlarni bo'lishi mumkin bo'lgan barcha variantlarini hisoblash uchun sarf bo'ladigan vaqt va zarur bo'ladigan hisoblash texnikasi resurslari bilan baholanadi.

Simmetrik blokli shifrlarda kalitlarni aniqlash uchun kriptanalitikka bir necha shifrmatn bloklari va unga mos keluvchi ochiq matn bloklari zarur bo'ladi. Agar kalit 8 bitdan iborat bo'lsa, u holda 8 bitli kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^8 ga teng, ya'ni 256 ta 8 bitli kalitlar ichidan aynan zarur bo'lgan kalitni saralash lozim. Ushbu holda saralashni yarmini bajargandan so'ng 50% ehtimollik bilan zarur kalitni topish mumkin.

Agar kalit uzunligi 56 bit bo'lsa, u holda kalitlarni bo'lishi mumkin bo'lgan barcha variantlari soni 2^{56} ga teng. Sekundiga miliion kalitni

Faraz qilaylik, $E_K(X)$ bu maxfiy kalitlarni generatsiya qilish uchun qo'llaniladigan, generatsiya qilingan K kalit orqali DES kriptografik algoritmidan foydalanib X matnini shifrlash bo'lsin. V_0 - 64 bitli boshlang'ich ketma-ketlik, T - vaqt nishoni bo'lsin. Tasodifiy R_i kalitni generatsiya qilishni quyidagicha bajarish mumkin:

$$R_i = E_K(E_K(T_i) \oplus V_i).$$



7.1-rasm. ANSI X9.17 standarti bo'yicha kalitlarni generatsiya qilish.

V_{i-1} ni generatsiya qilish :

$$V_{i-1} = E_K(E_K(T_i) \oplus R_i).$$

R_i ni DES kalitiga aylantirish uchun, undagi har bir sakkizinchi bitni o'chirish orqali erishish mumkin. Agar 64 bitli kalit kerak bo'ladigan bo'lsa, u holda R_i ni o'zgartirmasdan foydalanish mumkin. Agar 128 bitli kalit kerak bo'ladigan bo'lsa, u holda bir juft 64 bitli kalitlar yaratish va ularni birlashtirish lozim bo'ladi.

X9.17 standartiga asosan kalitlar 2 xil bo'ladi: kalitlarni shifrlash kalitlari va ma'lumotlarni shifrlash kalitlari. Kalitlarni shifrlash kalitlari yordamida kalitlarni tarqatish vaqtida boshqa kalitlar shifrlanadi.

§7.3. Simmetrik shifrlash algoritmlari uchun kalitli axboratlarni generatsiya qilish

Kriptografik algoritmlardan foydalanishda eng murakkab masalalardan biri kalitlarni generatsiya qilishdir. Bu holatda asosiy muammo yaratilayotgan kalitlarda ma'lum bir kriptografik xususiyatlarni mujassamlashtirishdir.

Simmetrik kalit uzunligi (bitlarda)	Asimmetrik kalit uzunligi (bitlarda)
56	384
64	512
80	768
112	1792
128	2304

§7.2. Seansli kalitlarni generasiya qilish

Foydalanuvchi paroli asosida seansli kalitlarni generasiya qilish. Seansli kalitlarni yaratishning keng tarqalgan usullaridan biri foydalanuvchi paroli asosida kalitlarni generasiya qilishdir. Foydalanuvchi paroli ustida kriptografik almashtirishlar bajariladi. Natija kalit sifatida qabul qilinadi. Keynichalik ushbu kalitni foydalanuvchi tarmoq trafiginı shifrlash uchun ishlatilishi mumkin.

Ushbu usulning yutug'i shundan iboratki, maxfiy kalitlarni saqlashga zarurat bo'lmaydi. Maxfiy kalitni yaratishda foydalanilgan parolni foydalanuvchi eslab yurishi yetarli.

Usulning kamchiligi shundaki, ushbu holatda raqibda lug'at yordamida hujum tashkil qilish imkoniyati paydo bo'ladi. Mazkur hujumning mohiyati eng katta ehtimolli so'zlarni saralash yo'li bilan raqib foydalanuvchi parolini aniqlashi mumkin. Chunki, parolni tanlashda ko'p hollarda esda oson saqlanishi mumkin bo'lgan so'zlardan yoki belgilar naboridan foydalaniladi.

Seansli kalitlarni generasiya qilishning X9.17 standarti. ANSI X9.17 standarti kalitlarni generasiya qilish usullarini aniqlaydi (8.1-rasm). Ushbu standart oson esda saqlanib qoladigan kalitlarni emas, balki seansli kalitlarni yoki psevdotasodifiy sonlarni generasiya qilishga mo'ljallangan. Kalitlarni generasiya qilishda DES kriptografik algoritmidan foydalaniladi, ammo uni o'rniga boshqa algoritmdan ham foydalanish mumkin.

keyinchalik oqimli shifratlarda 2 modul bo'yicha qo'shish yoki kalitlarni shakllantirishda boshlang'ich ketma-ketlik sifatida xizmat qilishi uchun ikkilik ko'rinishidagi ketma-ketliklar sifatida ifodalanadi.

§7.4. Asimmetrik (ochiq kalitli) shifrlash algoritmlari uchun kalitli axboratlarni generatsiya qilish

Ochiq kalitli shifrlash algoritmlari uchun kalitli axboratlarni generatsiya qilish simmetrik kriptotizimlarga nisbatan juda oddiy. Chunki, ochiq kalitli kriptotizimlarda maxfiy kalitlar ununig egasigagina tegishli bo'lib, ularni qandaydir aloqa kanali orqali uzatishga yoki boshqa foydalanuvchilarga tarqatishga hojat yo'q.

Asimmetrik kriptotizimlarda har bir foydalanuvchi o'zining ochiq va yopiq (maxfiy) kalitlar juftligiga ega. Xabarni jo'natuvchi xabarni qabul qiluvchining ochiq kalitlar juftligidan foydalanib, ma'lumotlarni shifrlab, aloqa kanali orqali jo'natadi. Shifrlangan ma'lumotni qabul qilgan foydalanuvchi o'zining yopiq kalitlar juftligidan foydalanib, sifratni dastlabki matnga o'giradi.

Foydalanuvchilarning ochiq kalitlar juftligi tarmoqdagi boshqa foydalanuvchilar ishlatishlari uchun ochiq holda e'lon qilinishi yoki biror ma'lumotlar bazasida saqlanishi mumkin. Shu sababli asimmetrik kriptotizimlar ochiq kalitli kriptotizimlar deb ham nomlanadi.

§7.5. Kalitlarni saqlash

Axborotni kriptografik himoyalashning ishonchli tizimini yaratishda birinchi navbatdagi asosiy masalalardan biri foydalanuvchining kalitini ish joyida ishonchli himoyasini ta'minlashdan iborat. Buzg'unchiga boshqalarning kalitiga ega bo'lishning oson yo'llari raqib xodimlarini o'z tomoniga og'dirish, viruslar va xotiraga to'g'ridan-to'g'ri murojaat qiladigan maxsus dasturiy vositalardan foydalanishdan iborat. Ushbu usullar kriptografik algoritmlarga hujum qilish uchun qimmatbaho hisoblash texnikasi vositalari va katta vaqtni talab qilmaydilar.

Kalitlarni generasiya qilishning 2 xil usuli mavjud: determinallashgan va nodeterminallashgan.

Determinallashgan usul. Ushbu usullarning mohiati kichik uzunlikdagi tasodifiy ketma-ketliklardan statistik xususiyatlari bo'yicha dastlabki ketma-ketliklardan uncha farq qilmaydigan katta uzunlikdagi psevdotasodifiy ketma-ketliklarni shakllantirishdan iborat. Psevdotasodifiy ketma-ketliklarni shakllantirishning eng keng tarqalgan usullaridan biri chiziqli teskari bog'lanishli siljitish registrlaridan foydalanish. Ular chiziqli rekurrent ketma-ketliklar vositasida ifodalanib, ulardan har doim ham psevdotasodifiy kalitlar ketma-ketligi generatori sifatida foydalanish mumkin emas. Shu sababli psevdotasodifiy xarakterga va fizikaviy tabiat (muskullarning harakati, kirish/chiqish qurilmalari bilan ishlashda foydalanuvchining ularga murojaat qilish vaqti) ga ega bo'lgan jarayonlardan foydalanish keng tarqalmoqda.

Ixtiyoriy holatda ham kalitlarni generasiya qilishda quyidagilarga e'tibor qilish maqsadga muvofiq:

- k belgidan tashkil topgan ketma-ketlik (k -gramma) ni paydo bolish chastotasini χ -kvadrat mezoniga tekshirish;
- natijalar chastotasini umumlashgan χ -kvadrat mezoniga tekshirish;
- markirovka qilishning minimal va maksimal qiymatlarini tekshirish;
- ustma-ust tushmaslik oraliqlari uzunliklarini berilgan diapazon bilan solishtirish;
- monotonlikka tekshirish.

Nodeterminallashgan usul. Natijalari keyinchalik kalitlarni generasiya qilishda qo'llaniladigan tasodifiy fizik jarayonlar ushbu usullar asosini tashkil qiladi. Tasodifiy natijalar hosil qilishga oddiy misol sifatida o'yin suyaklari yoki tangani tashlashni ko'rsatish mumkin. Kichik unumdorligi sababli amaliyotda ulardan foydalanish maqsadga muvofiq bo'lmasa-da, nazariy jihatdan ular kalitlar ketma-ketligi generatori sifatida xizmat qilishi mumkin.

Hozirgi vaqtda chiquvchi ketma-ketliklari tasodifiy tarqalgan fizikaviy shovqin generatorlari (masalan, shovqin soluvchi diodlar, impulsli generatorlar, Geyger hisoblagichlari) keng qo'llanilmoqda. Ushbu asbob yoki qurilmalardan olingan signallar raqamlashtiriladi. Ular

autentikasiya qilish, undan so'ng kriptografik protokollardan foydalanishga asoslangan.

Kalitlarni tarqatish jarayoniga quyidagi talablar qo'yiladi:

1. axborot almashinuvida ishtirok etuvchi har bir ishtirokchi protokollardan foydalanish jarayonida kalitlarni maxfiylikka ishonch hosil qilishi lozim;

2. kalit kimga mo'ljallangan bo'lsa, o'sha ishtirokchi kalitni qabul qilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (qabul qilganligini tasdiq'i talab qilinadi);

3. kalit kimga jo'natilishi lozim bo'lsa, o'sha ishtirokchiga kalit jo'natilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (tomonlar autentikasiyasi talab qilinadi).

Kalitlarni tarqatishning 2 xil protokoli mavjud:

- generasiya qilingan kalitlarni tarqatish protokollari;
- kalitlarni birgalikda shakllantirish protokollari.

Ikki va undan ortiq ishtirokchilar o'rtasida kalitlarni tarqatish protokollari va sxemalari ham turlicha bo'ladi. Ko'p ishtirokchilar o'rtasida kalitlarni tarqatishda markazlashtirilgan kalitlarni tarqatish sxemasidan foydalaniladi.

Bundan tashqari foydalanuvchilar bir-biriga ishongan va ishonmagan hollarda turli xil protokollardan foydalinaladi. Foydalanuvchilar bir-biriga ishongan hollarda simmetrik va ochiq kalitli kriptotizimlardan foydalanishlari mumkin. Foydalanuvchilar bir-biriga ishonmagan hollarda faqatgina ochiq kalitli kriptotizimlarga asoslangan protokollardan foydalanishlari mumkin.

Seansli kalitlarni tarqatishning muvaffaqiyatli yechimlaridan biri gibrid kriptotizimlardan foydalanishdir. Bunda ma'lumotlarni shifrlashda simmetrik, kalitlarni tarqatishda ochiq kalitli kriptotizimlardan foydalanish mumkin. Shu sababli gibrid kriptotizimlar simmetrik kriptotizimlarga xos bo'lgan yuqori tezlikda shifrlash, ochiq kalitli kriptotizimlarga xos bo'lgan kalitlarni qulay tarzda tarqatish bilan xarakterlanadi.

Foydalanuvchi ish joyida kalitlarni saqlashni ishonchli tashkil qilishning asosiy usullarini quyidagicha keltirish mumkin:

- kalitlarni saqlashda ishlatiladigan xotirani ruxsat etilmagan kirishlardan himoyalaydigan kript Qurilmalardan foydalanish;
- foydalanuvchi shaxsiy kompyuterida kalitlarni bevosita shifrlangan holatda saqlash;
- kalitlarni saqlashda tashqi Qurilmalardan foydalanish.

Birinci usul eng **ishonchli** bo'sa-da, foydalanuvchida har doim ham bunday Qurilmalar bilan ishlashning imkoniyati yo'q. Bundan tashqari bunday kript Qurilmalarning xotirasi uncha katta bo'lmaydi. Shu sababli bu turdagi Qurilmalarda amalda shifrlash kalitlari yoki seans yoxud fayl (direktoriya) lar kalitlari saqlanadi.

Ikkinchi usulni batafsil izohlashning hojati yo'q. Bunday tarzda ko'pchilik hollarda fayl (direktoriya) larni shifrlash kalitlari saqlanadi.

Uchinchi usul hozirgi kunda eng istiqbolli usullardan biri hisoblanadi. Oxirgi vaqtlarda kalitli axborotlarni uzoq muddatda saqlash imkoniyatiga ega bo'lgan ko'plab Qurilmalar paydo bo'lmoqda. Bunday Qurilmalarni himoyalash tashkiliy usullar bilan oson hal qilinadi. Boz ustiga mazkur Qurilmalarni zamonaviy hisoblash texnikasi vositalari bilan birgalikda foydalanilish imkoniyati mavjud. Shu sababli bunday Qurilmalarni amaliyotda qo'llash diapazoni kengayib bormoqda. Kalitli axborotlarni saqlashga mo'ljallangan Qurilmalar sifatida magnit kartalari, egiluvchan magnitli disklar, elektron plastikli kalitlar va elektron karta (smart-cards) larni ko'rsatish mumkin. Keltirilganlardan eng istiqbollisi smart-kartalalar bo'lib, ular kalitlarni tashuvchisidan tashqari kriptosxemalarni analga oshiruvchi texnik vositalar sifatida ham ishlatilishi mumkin.

§7.6. Kalitlarni tarqatish sxemalari

Simmetrik kriptotizimlarda kalitlarni tarqatish himoyalangan aloqa kanalidan va kriptografik protokollardan foydalanishga asoslangan. Ochiq kalitli va gibridli kriptotizimlarda kalitlarni tarqatish ochiq kalitlarni

autenfikasiya qilish, undan so'ng kriptografik protokollardan foydalanishga asoslangan.

Kalitlarni tarqatish jarayoniga quyidagi talablar qo'yiladi:

1. axborot almashinuvda ishtirok etuvchi har bir ishtirokchi protokollardan foydalanish jarayonida kalitlarni maxfiylikka ishonch hosil qilishi lozim;

2. kalit kimga mo'ljallangan bo'lsa, o'sha ishtirokchi kalitni qabul qilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (qabul qilganligini tasdig'i talab qilinadi);

3. kalit kimga jo'natilishi lozim bo'lsa, o'sha ishtirokchiga kalit jo'natilganligiga har bir ishtirokchi ishonch hosil qilishi lozim (tomonlar autenfikasiyasi talab qilinadi).

Kalitlarni tarqatishning 2 xil protokoli mavjud:

- generasiya qilingan kalitlarni tarqatish protokollari;
- kalitlarni birgalikda shakllantirish protokollari.

Ikki va undan ortiq ishtirokchilar o'rtasida kalitlarni tarqatish protokollari va sxemalari ham turlicha bo'ladi. Ko'p ishtirokchilar o'rtasida kalitlarni tarqatishda markazlashtirilgan kalitlarni tarqatish sxemasidan foydalaniladi.

Bundan tashqari foydalanuvchilar bir-biriga ishongan va ishonmagan hollarda turli xil protokollardan foydalinaladi. Foydalanuvchilar bir-biriga ishongan hollarda simmetrik va ochiq kalitli kriptotizimlardan foydalanishlari mumkin. Foydalanuvchilar bir-biriga ishonmagan hollarda faqatgina ochiq kalitli kriptotizimlarga asoslangan protokollardan foydalanishlari mumkin.

Seansli kalitlarni tarqatishning muvaffaqiyatli yechimlaridan biri gibrid kriptotizimlardan foydalanishdir. Bunda ma'lumotlarni shifrlashda simmetrik, kalitlarni tarqatishda ochiq kalitli kriptotizimlardan foydalanish mumkin. Shu sababli gibrid kriptotizimlar simmetrik kriptotizimlarga xos bo'lgan yuqori tezlikda shifrlash, ochiq kalitli kriptotizimlarga xos bo'lgan kalitlarni qulay tarzda tarqatish bilan xarakterlanadi.

Foydalanuvchi ish joyida kalitlarni saqlashni ishonchli tashkil qilishning asosiy usullarini quyidagicha keltirish mumkin:

- kalitlarni saqlashda ishlatiladigan xotirani ruxsat etilmagan kirishlardan himoyalaydigan kript Qurilmalardan foydalanish;
- foydalanuvchi shaxsiy kompyuterida kalitlarni bevosita shifrlangan holatda saqlash;
- kalitlarni saqlashda tashqi Qurilmalardan foydalanish.

Birinchi usul eng ishonchli bo'sa-da, foydalanuvchida har doim ham bunday Qurilmalar bilan ishlashning imkoniyati yo'q. Bundan tashqari bunday kript Qurilmalarning xotirasi uncha katta bo'lmaydi. Shu sababli bu turdagi Qurilmalarda amalda shifrlash kalitlari yoki seans yoxud fayl (direktoriya) lar kalitlari saqlanadi.

Ikkinchi usulni batafsil izohlashning hojati yo'q. Bunday tarzda ko'pchilik hollarda fayl (direktoriya) larni shifrlash kalitlari saqlanadi.

Uchunchi usul hozirgi kunda eng istiqbolli usullardan biri hisoblanadi. Oxirgi vaqtlarda kalitli axborotlarni uzoq muddatda saqlash imkoniyatiga ega bo'lgan ko'plab Qurilmalar paydo bo'lmoqda. Bunday Qurilmalarni himoyalash tashkiliy usullar bilan oson hal qilinadi. Boz ustiga mazkur Qurilmalarni zamonaviy hisoblash texnikasi vositalari bilan birgalikda foydalanilsh imkoniyati mavjud. Shu sababli bunday Qurilmalarni amaliyotda qo'llash diapazoni kengayib bormoqda. Kalitli axborotlarni saqlashga mo'ljallangan Qurilmalar sifatida magnit kartalari, egiluvchan magnitli disklar, elektron plastikli kalitlar va elektron karta (smart-cards) larni ko'rsatish mumkin. Keltirilganlardan eng istiqbollisi smart-kartalar bo'lib, ular kalitlarni tashuvchisidan tashqari kriptoxemalarni amalga oshiruvchi texnik vositalar sifatida ham ishlatilishi mumkin.

§7.6. Kalitlarni tarqatish sxemalari

Simmetrik kriptotizimlarda kalitlarni tarqatish himoyalangan aloqa kanalidan va kriptografik protokollardan foydalanishga asoslangan. Ochiq kalitli va gibriddli kriptotizimlarda kalitlarni tarqatish ochiq kalitlarni

KTM tomonidan kalitlarni qayd qilish jurnali (alohida fayl) da kalitlar haqidagi ma'lumotlar kiritilib boriladi. Ushbu jurnalda odatda quyidagilar aks etgan bo'ladi:

1. kalitlarni generatsiya qilinish sanasi;
2. kalitlarni turi va nomi;
3. kalitlarni amal qilish muddati;
4. kalitlardan foydalanuvchi abonentlar ro'yxati;
5. kalitlarni o'z foydalanuvchisiga jo'natilganligi haqidagi ma'lumotlar;
6. kalitlarni qabul qilinganligi haqidagi foydalanuvchilarning tasdiqlari va shunga o'xshash ma'lumotlar.

KTMning lavozimli, kalitlarni saqlash va kalit tashuvchilaridan foydalanishga javobgar xodimlarining kalitlarga ruxsati bo'lishi mumkin. Shuningdek, kalitlarga ruxsat quyida keltirigan texnik tadbirlar bilan cheklanishi mumkin:

- 1) kalitlarni generatsiya qilish jarayoni ruxsat etilmagan kirishlardan himoyalangan holda EHM yordamida avtomatik tarzda amalga oshirilishi lozim;
- 2) seansli kalitlar shakllantirilish jarayonida foydalanuvchilardan yashirin tarzda amalga oshirilishi lozim;
- 3) kalitlar ochiq holatda saqlanmasligi lozim;
- 4) kalitlar faqatgina avtonom tashuvchilarda yozilishi (ko'chirilishi) lozim.

Bayon etilgan KTM sxemasining yutug'i shundaki, abonentlar sifatli kalitlarni generatsiya qilish uchun KTM kabi zamonaviy qurilmalarga, malakali mutaxassislariga ega emas. Kamchiligi esa agar KTM ishonchni yo'qotsa, ushbu markaz xizmat ko'rsatayotgan barcha abonentlar kalitlarining maxfiyligi shubha ostigai qoladi va ular kalitlar masalasida boshqa KTMga murojaat qilishlariga to'g'ri keladi.

§7.7. Kalitlarni markazlashgan tarqatish

Faraz qilaylik, axborot almashiniuv tizimida N ta foydalanuvchi mavjud. Ushbu tizimdagi A va B foydalanuvchilar axborot almashishlari uchun K seans kalitiga ehtiyoj sezmoqdalar. Mazkur axborot almashiniuv tizimida odatdagi foydalanuvchilardan tashqari kalitlarni tarqatish markazi (KTM) deb nomlanuvchi ishonchli markaz ham ishtirok etmoqda.

KTM har bir abonent (foydalanuvchi) uchun turli K_i ($i = \overline{1, N}$) maxfiy kalitlarni generatsiya qiladi va himoyalangan aloqa kanali orqali ushbu kalitlar bilan abonentlarni ta'minlaydi. Ushbu mazkur K_i ($i = \overline{1, N}$) maxfiy kalitlar bosh kalitlar deb nomlanadi va ulardan abonentlar KTM bilan aloqa qilishda foydalanishadi.

Seansli kalitlarni uzatishda shifrlashning maxsus algoritmi ishlatiladi. $E_K(x)$ orqali ushbu shifrlash algoritmidan foydalanib, x ma'lumotni K kalit yordamida shifrlash tushuniladi.

Agar A_i va A_j abonentlar o'zaro maxfiy aloqa o'rnatmoqchi bo'lsalar, ular KTMga murojaat qilishadi. KTM esa ular uchun K_{ij} umumiy seans kalitini ishlab chiqadi. KTM A_i abonentga $E_{K_i}(K_{ij})$, A_j abonetga $E_{K_j}(K_{ij})$ ni ochiq aloqa kanali orqali jo'natadi. Qabul qilingan ma'lumotlarni A_i va A_j abonentlar dastlabki matnga o'girib, K_{ij} umumiy seans kalitiga ega bo'lishadi.

Bu yerda shifrlashda qo'llanilgan E kriptotalgoritmi ishonchli, shu sababli K_i va K_j kalitlarni bilmagan buzg'unchi K_{ij} umumiy seans kalitini hosil qilolmaydi yoki uni boshqasi bilan almashtiriolmaydi. Agar KTMdan foydalanuvchi abonentlar soni ko'p bo'lsa, ushbu KTM asosida ierarxik tomoyil bo'yicha bir necha ishonchli markazlar tashkil qilinishi mumkin. Natijada bosh KTM va uning mintaqaviy markazlari hosil qilinishi mumkin. Mintaqaviy KTMlar o'z guruh (hudud) laridagi abonentlarga xizmat ko'rsatishlari mumkin. Turli xil guruhdagi abonentlar bir-birlari bilan aloqa o'rnatmoqchi bo'lsalar, bosh KTM tomonidan ularga seans kalitlari taqdim qilinadi.

Birinchi qadamda A abonent tomonidan T isonchli markazga kalitni uzatish va A abonentni T tomonidan autentifikasiyasilanishi amalga oshirilgan.

Ikkinchi qadamda T isonchli markazni B abonentga kalit uzatishi va T markazni B tomonidan autentifikasiyasilanishi amalga oshirilgan. Bundan tashqari T markaz A abonent tomonidan kalit uzatilganligini B ga xabar qildi. Har ikki qadamda ham buzg'unchi ushlab olingan eski ma'lumotlardan foydalanishiga yo'l qo'ymaslik maqsadida shifrlangan vaqt nishonlaridan foydalanilgan.

Ushbu protokolda A abonentni T tomonidan autentifikasiyasilanishi amalga oshirilgan. Ammo, kalitni muvaffaqiyatli qabul qilinganligi tasduqlovchi va B abonentni A tomonidan autentifikasiyasilanishi amalga oshiruvchi qadamlar nazarda tutilmagan.

§7.10. Yahalom protokoli

1. $A \rightarrow B: A, R_A;$
2. $B \rightarrow T: B, E_B(A, R_A, R_B);$
3. $T \rightarrow A: E_A(B, K, R_A, R_B), E_B(A, K);$
4. $A \rightarrow B: E_B(A, K), G = E_K(R_B).$

5. B: $G = E_K(R_B)$ ekanligini tekshirib ko'radi, natiija ijobiy bo'lsa, B K kalitni qabul qiladi.

Ushbu protokolning oldingi protokoldan farqi shundaki, unda xabar almashinuvuga tashabbuskor shaxs to'g'ridan-to'g'ri o'z hamkoriga murojaat qiladi (1-qadam) va u yakuniy kalit almashinuvuni amalga oshiradi (4-qadam). Ikkinchi tomondan seansli kalit T markaz tomonidan amalga oshiriladi. Shuningdek, vaqt nishonlari o'rniga bir martalik tasodifiy sonlar ishlatiladi. Bu esa bu protokolda ishlatiluvchi barcha ma'lumotlardan bir marta foydalanishni anglatadi.

A abonent orqali B abonentga kalitni uzatilishi B abonent tomonidan A abonentni autentifikasiyalashni ta'minlaydi. Haqiqatan ham, agar buzg'unchi o'zini A abonent o'rnida tutayotgan bo'lsa, u A abonentning kalitiga ega emasligi sababli 3-qadamda $E_A(B, K, R_A, R_B)$ ni dastlabki

§7.8. Simmetrik kriptografiyadan foydalanib, ishonchli markaz tomonidan maxfiy kalitlarni tarqatish protokoli

Agar kalit foydalanuvchi tomonidan generatsiya qilinsa va uni ishonchli markaz boshqa foydalanuvchi yetkazib bersa, kalitning xavfsizligiga tahdid kuchayadi. Shuningdek, seansli kalitning xavfsizligi u shifrlanadigan shifrlash algoritmining ishonchliligiga ham bog'liq. Ammo, buzg'unchi kalitni uzatish protokolida aralashishi yoki o'zini qonuniy foydalanuvchi sifatida tutib, seansli kalitni o'zgartirish maqsadida o'zi shunday protokolni o'ylab topishi mumkin. Shu sababli abonentlarni o'zaro autentifikatsiyasiga asoslangan kalitlarni uzatishning mukammal protokoliga zaruriyat paydo bo'ladi.

Mavzuni bayon qilishda A abonent B abonentga kalitni uzatish ishonchli markaz T orqali amalga oshiriladi deb faraz qilinadi hamda quyidagi belgilashlardan foydalaniladi:

E_A, E_B orqali mos holda A va B abonentlarning bosh kalitlari bilan shifrlash ifodalanadi.

K, I, L - mos holda maxfiy seans kalitini, uning tartib nomerini va umri (foydalanish muddati) ni anglatadi.

T_A, T_B - mos holda A va B abonentlar tomonidan yaratilgan vaqt nishonlarini bildiradi.

R_A, R_B - mos holda A va B abonentlar tomonidan tasodifiy tanlangan sonlarni anglatadi.

X, Y - X va Y sonlarini konkatenasini bildiradi.

Shart bo'lmagan parametrlar yulduzcha bilan X^* kabi belgilanadi.

§7.9. Wide-Mouth Frog protokoli

Ushbu protokol kalitni ishonchli markaz orqali uzatishga misol bo'ladi. U quyida keltirilgan tartibda amalga oshiriladi:

1. $A \rightarrow T: A, E_A(T_A, B, K);$

2. $T \rightarrow B: E_B(T_B, A, K).$

2-3 qadamlarda A abonent K kalit bilan shifrlangan xabardan $E_B(K, A)$ xabarni olib, uni B abonentga uzatish natijasida B abonent tomonidan autentifikasiyalanadi.

B abonent A abonent tomonidan autentifikasiyalanmaydi. Buzg'unchi o'zini A abonent sifatida namoyon qilib, 4-qadamda ixtiyoriy tasodifiy sonni B abonentga jo'natishi mumkin. Ammo, bu unga hech narsa bermaydi, chunki u maxfiy kalitni bilmaydi.

4-5 qadamlar B abonentga A abonent ham o'zi qabul qilgan aynan K kalitni olganligini tasdiqlaydi. Ammo, buzg'unchi o'zini A abonent sifatida namoyon qilib, B abonentga eski K' kalitni taqdim qilishi mumkin. Haqiqatan ham protokolda B va T bevosita muloqat qilishmaydi. Shu sababli M (buzg'unchi) 3-qadamdan boshlab B abonent bilan muloqat qilishni boshlaydi:

M(A nomidan) → B: $E_B(K', A)$;

(Ushbu xabarni A abonent B abonentga eski K' kalitni jo'natgan vaqtida tutib olgan edi.) B abonent qabul qilingan kalit oldin ishlatilgan yoki ishlatilmaganligini tekshirmasa, u holda B uni to'g'ri kalit sifatida qabul qiladi va A abonentga xabar jo'natadi:

4. **B → A:** $E_K(R_B)$;

B abonent tomonidan g'alati xabarlar kelayotgani haqida A abonent T markazga xabar qilmasligi uchun M buzg'unchi B abonent tomonidan A abonentga jo'natilayotgan barcha xabarlarni blokirovka qilishi lozim bo'ladi.

5. **M(A nomidan) → B:** $E_K(R_B - 1)$.

Shunday qilib, B abonent tomonidan unga uzatilgan barcha kalitlar jurnalda qayd qilib borilgan hollardagina ushbu protokolni ishlatish mumkin.

§7.12. Otvey-Riis protokoli

1. **A → B:** $I, A, B, E_A(R_A, I, A, B)$;

2. **B → T:** $I, A, B, E_A(R_A, I, A, B), E_B(R_B, I, A, B)$;

3. **T → B:** $I, E_A(K, R_A), E_B(K, R_B)$;

4. **B → A:** $I, E_A(K, R_A)$.

matnga o'gira olmaydi. Natijada undan R_B va K ni hosil qilolmaydi. Demakki, xabarni ham hosil qilolmaydi. Uni o'rninga boshqa xabarni jo'natsa, B abonent ushbu xabarni K kalit bilan dastlabki matnga o'girib, natija R_B bir xil emasligini ko'rib, buzg'unchi jo'natgan K kalitdan foydalanishni rad etadi.

B abonentni A abonent tomonidan autentifikasiyalanishi 2-3 qadamlarda T markaz orqali shifrlangan ma'lumotlarni uzatish yordamida amalga oshiriladi.

B abonent 4-qadamda qabul qiladigan $E_K(R_B)$ nafaqat A abonentni B abonent tomonidan autentifikasiyalanishini, balki axborotni uzatish jarayonida o'zgartirilmaganligini tekshirishni ham ta'minlaydi.

Xulosa sifatida shuni aytish mumkinki, ushbu protokol nafaqat kalitni uzatishni amalga oshiradi, balki xabarlardan takroran foydalanishga to'sqinlik qilib, B abonentga A abonent olgan kalitni olganligiga ishonch hosil qilish imkonini yaratadi. Protokolda xuddi shunga o'xshash tekshirishni A abonent ham o'tkazish imkoniyati mavjud emas.

§7.11. Nidxem-Shreder protokoli

Ushbu protokol A abonentni aldash maqsadida eski ma'lumotlarni takroran uzatish asosidagi hujumga to'sqinlik qiladi. Protokoldagi ixtiyoriy ma'lumotni qabul qilgan shaxs olingan ma'lumotni kutilayotgan ma'lumotga mosligini tekshirib ko'rishi lozim. Agar protokolni bajarilish vaqtida biror bir ziddiyatga duch kelinsa, u holda bu protokolni bajarilishini to'xtatish lozim va bu haqida boshqa ishtirokchilarga ham ma'lum qilishi kerak.

Protokol quyidagi tartibda amalga oshiriladi:

1. $A \rightarrow T$: A, B, R_A ;
2. $T \rightarrow A$: $E_A(R_A, B, K, E_B(K, A))$;
3. $A \rightarrow B$: $E_B(K, A)$;
4. $B \rightarrow A$: $E_K(R_B)$;
5. $A \rightarrow B$: $E_K(R_B - 1)$.

Asimmetrik kriptotizimlarga asoslangan axborotni uzatishning protokollari bosh kalitni yoki seans kalitini uzatishda himoyalangan kanal sifatida ishlatilishi mumkin. Bu turdagi kriptotizimlarning kamchiligi shifrlash jarayonining sekinligi va ixtoyoriy uzunlikdagi qiymat bilan berilgan ma'lumot kalit sifatida qabul qilinmasligi bilan xarakterlanadi. Kalitlarni uzatishda shifrlanadigan ma'lumot uncha katta hajmga ega bo'lmasligi e'tiborga olinsa, birinchi kamchilik unchalik ahamiyatga ega emas. Asimmetrik kriptotizimlarga asoslangan protokollardan foydalanishni qulayligi ikkinchi kamchilikni to'liq qoplaydi.

§7.14. Shamirning kalitsiz protokoli

Ushbu protokolning bardoshligi diskret logarifmlash masalasining murakkabligiga asoslangan.

Protokolda quyidagi parametrlardan foydalaniladi:

p – katta tub son;

K – seans kaliti.

Protokolni amalga oshirish quyidagi qadamlrga asoslangan:

1. $A \rightarrow B: x_1 = K^a \pmod p$, bu yerda $a: 1 < a < p-1$ oraliqdan olingan tasodifiy son;
2. $B \rightarrow A: x_2 = (x_1)^b \pmod p$, bu yerda $b: 1 < b < p-1$ oraliqdan olingan tasodifiy son;
3. $A \rightarrow B: x_3 = (x_2)^{a^{-1} \pmod{p-1}} \pmod p$;
4. $B: (x_3)^{b^{-1} \pmod{p-1}} \pmod p = K$ ni hisoblaydi.

Ushbu protokol natijasida B abonent umumiy bo'lgan K kalitga ega bo'ladi.

Shuni ta'kidlash lozimki, a va b sonlari aloqa kanali orqali uzatilmasligi lozim, ular protokol tugaguncha maxfiy tutiladi va protokol tugagandan so'ng yuqotiladi.

Protokolni yutug'i sifatida abonentlarning ochiq va maxfiy kalitlarini ishlatilmasligi hamda ishonchli markaz, himoyalangan aloqa kanali, kalitlarni autentifikasiya qilishga zaruratning yo'qligi bilan xarakterlanadi.

Protokoldagi ixtiyoriy ma'lumotni qabul qilgan shaxs olingan ma'lumotni kutilayotgan ma'lumotga mosligini tekshirib ko'rishi lozim.

2-qadamda $E_A(R_A, I, A, B)$, $E_B(R_B, I, A, B)$ xabarlarini T markaz dastlabki matnga o'girib, ulardan I, A, B parametrlarni hosil qilishi va ularni ochiq holda jo'natilganligi bilan teng yoki teng emasligini tekshirib ko'rishi lozim bo'ladi. Agar parametrlar qiymatlari teng bo'lmasa, T markaz protokolni to'xtatishi va abonentlarga qaytadan protokoldan o'tishlarini so'rab, xabar qilishi kerak.

3-qadamda B abonent $E_B(K, R_B)$ xabarni dastlabki matnga o'girib, undan R_B ni hosil qilishi lozim. Agar u 2-qadamda generatsiya qilingan R_B bilan teng bo'lmasa, B abonent protokolni to'xtatishi va unga taqdim qilingan K seans kalitini rad etishi lozim.

B abonent 3-qadamda qanday ish tutgan bo'lsa xuddi shu ishni A abonent 4-qadamda amalga osirishi lozim.

Ushbu protokol ishlatigan, eski xabarlardan takroran foydalanishga to'sqinlik qiladi (ochiq va shifrlangan holda qatnashuvchi tasodifiy sonlar va I soni aynan to'sqinlik qiladi). Shuningdek, buzg'unchiga B abonentga o'zini A abonent sifatida ko'rsatishiga imkon bermaydi.

Protokolda A va B abonentlar o'zi qabul qilgan aynan K kalitni boshqasi ham olganligiga ishonch hosil qiladigan qadamlar, ya'ni Nidxem-Shreder protokolidagi 4-5 qadamlar kabi qadamlar mavjud emas.

§7.13. Ikki kalitli kriptografiyadan foydalanib, kalitlarni tarqatish

Maxfiy kalitlarni tarqatishda simmetrik shifrlash tizimlarining imkoniyatlari cheklangan. Shifrlash va seans kalitlarini uzatishga kirishish uchun avval himoyalangan aloqa kanali orqali bosh kalitni uzatish lozim bo'ladi. Aks holda qabul qiluvchi seans kalitini dastlabki matnga o'girolmaydi.

Ikkikalitli – asimmetrik kriptografiyadan foydalanilganda axborotlarni shifrlashda qabul qiluvchining maxfiy kalitidan foydalanishga hojat yo'q. Buning uchun ochiq aloqa kanali orqali yuboriladigan qabul qiluvchining ochiq kaliti yetarli bo'ladi.

Asimmetrik kriptotizimlarga asoslangan axborotni uzatishning protokollari bosh kalitni yoki seans kalitini uzatishda himoyalangan kanal sifatida ishlatilishi mumkin. Bu turdagi kriptotizimlarning kamchiligi shifrlash jarayonining sekinligi va ixtoyoriy uzunlikdagi qiymat bilan berilgan ma'lumot kalit sifatida qabul qilinmasligi bilan xarakterlanadi. Kalitlarni uzatishda shifrlanadigan ma'lumot uncha katta hajmga ega bo'lmisligi e'tiborga olinsa, birinchi kamchilik unchalik ahamiyatga ega emas. Asimmetrik kriptotizimlarga asoslangan protokollardan foydalanishni qulayligi ikkinchi kamchilikni to'liq qoplaydi.

§7.14. Shamirning kalitsiz protokoli

Ushbu protokolning bardoshligi diskret logarifmlash masalasining murakkabligiga asoslangan.

Protokolda quyidagi parametrlardan foydalaniladi:

p – katta tub son;

K – seans kaliti.

Protokolni amalga oshirish quyidagi qadamlrga asoslangan:

1. $A \rightarrow B: x_1 = K^a \pmod p$, bu yerda $a: 1 < a < p-1$ oraliqdan olingan tasodifiy son;
2. $B \rightarrow A: x_2 = (x_1)^b \pmod p$, bu yerda $b: 1 < b < p-1$ oraliqdan olingan tasodifiy son;
3. $A \rightarrow B: x_3 = (x_2)^{a^{-1} \pmod{p-1}} \pmod p$;
4. $B: (x_3)^{b^{-1} \pmod{p-1}} \pmod p = K$ ni hisoblaydi.

Ushbu protokol natijasida B abonent umumiy bo'lgan K kalitga ega bo'ladi.

Shuni ta'kidlash lozimki, a va b sonlari aloqa kanali orqali uzatilmisligi lozim, ular protokol tugaguncha maxfiy tutiladi va protokol tugagandan so'ng yuqotiladi.

Protokolni yutug'i sifatida abonentlarning ochiq va maxfiy kalitlarini ishlatilmisligi hamda ishonchli markaz, himoyalangan aloqa kanali, kalitlarni autentifikasiya qilishga zaruratning yo'qligi bilan xarakterlanadi.

Protokoldagi ixtiyoriy ma'lumotni qabul qilgan shaxs olingan ma'lumotni kutilayotgan ma'lumotga mosligini tekshirib ko'rishi lozim.

2-qadamda $E_A(R_A, I, A, B)$, $E_B(R_B, I, A, B)$ xabarlarni T markaz dastlabki matnga o'girib, ulardan I, A, B parametrlarni hosil qilishi va ularni ochiq holda jo'natilganligi bilan teng yoki teng emasligini tekshirib ko'rishi lozim bo'ladi. Agar parametrlar qiymatlari teng bo'lmasa, T markaz protokolni to'xtatishi va abonentlarga qaytadan protokoldan o'tishlarini so'rab, xabar qilishi kerak.

3-qadamda B abonent $E_B(K, R_B)$ xabarni dastlabki matnga o'girib, undan R_B ni hosil qilishi lozim. Agar u 2-qadamda generasiya qilingan R_B bilan teng bo'lmasa, B abonent protokolni to'xtatishi va unga taqdim qilingan K seans kalitini rad etishi lozim.

B abonent 3-qadamda qanday ish tutgan bo'lsa xuddi shu ishni A abonent 4-qadamda amalga osirishi lozim.

Ushbu protokol ishlatigan, eski xabarlardan takroran foydalanishga to'sqinlik qiladi (ochiq va shifrlangan holda qatnashuvchi tasodifiy sonlar va I soni aynan to'sqinlik qiladi). Shuningdek, buzy'unchiga B abonentga o'zini A abonent sifatida ko'rsatishiga imkon bermaydi.

Protokolda A va B abonentlar o'zi qabul qilgan aynan K kalitni boshqasi ham olganligiga ishonch hosil qiladigan qadamlar, ya'ni Nidxem-Shreder protokolidagi 4-5 qadamlar kabi qadamlar mavjud emas.

§7.13. Ikki kalitli kriptografiyadan foydalanib, kalitlarni tarqatish

Maxfiy kalitlarni tarqatishda simmetrik shifrlash tizimlarining imkoniyatlari cheklangan. Shifrlash va seans kalitlarini uzatishga kirishish uchun avval himoyalangan aloqa kanali orqali bosh kalitni uzatish lozim bo'ladi. Aks holda qabul qiluvchi seans kalitini dastlabki matnga o'girolmaydi.

Ikkikalitli – asimmetrik kriptografiyadan foydalanilganda axborotlarni shifrlashda qabul qiluvchining maxfiy kalitidan foydalanishga hojat yo'q. Buning uchun ochiq aloqa kanali orqali yuboriladigan qabul qiluvchining ochiq kaliti yetarli bo'ladi.

3. A: $K=(\alpha^y)^x \bmod p$ ni hisblaydi;

4. B: $K=(\alpha^x)^y \bmod p$ ni hisblaydi.

Natijada Ava B umumiy seans kalitini hosil qilishadi. Protokollarning Shamir protokoli kabi yutuq va kamchiliklarga ega. Shamir protokollari uchun ushbu protokol ham «o'rtadagi odam» hujumiga nisbatan zaf. Hujum hujumni bartaraf etish uchun Shamir protokoli kabi har aktsiyat o'zining har bir xabarlariga elektron imzo qo'yishlari lozim bo'ladi.

Diffi-Xellman protokolining modifikatsiyasiga misol keltirish mumkin. Buning uchun quyidagi parametrlarni qo'shimcha tarzda kiritib lozim bo'ladi:

$S_B(X)$ – B ochiq kalitdan foydalanib, X xabarni ochig'iga qo'yadi;

$E_K(X)$ – X xabarni simmetrik kriptotizimdan foydalanib K kalit bilan shifrlash. Natijada Diffi-Xellman modifikatsiyalangan protokollari quyidagicha bo'ladi:

1. A \rightarrow B: $\alpha^x \bmod p$ (bu yerda x – tasodifiy maxfiy son);

2. B: y – tasodifiy maxfiy sonni tanlab, $K=(\alpha^x)^y \bmod p$ ni hisoblaydi;

3. B \rightarrow A: $\alpha^y \bmod p$, $E_K(S_B(\alpha^x \bmod p, \alpha^y \bmod p))$;

4. A: $K=(\alpha^y)^x \bmod p$ ni hisoblaydi, $E_K(S_B(\alpha^x \bmod p, \alpha^y \bmod p))$ ni dastlabki matnga o'girib, imzoni tekshiradi. Agar imzo qalbaki bo'lsa, protokollari to'xtadi va K kalitni rad etadi. Agar imzo haqiqiy bo'lsa, 5-qadamni bajaradi.

5. A \rightarrow B: $E_K(S_A(\alpha^x \bmod p, \alpha^y \bmod p))$;

6. B: $S_A(\alpha^x \bmod p, \alpha^y \bmod p)$ ni dastlabki matnga o'girib, imzoni tekshiradi. Agar imzo qalbaki bo'lsa, K kalitni rad etadi.

Ushbu protokol tomonlar autentifikatsiyasi (raqamli imzo vositasida) va kalit qabul qilinishini tasdiqlash (shifrlash yordamida) o'zida mujassam etgan. Protokollari qo'llaniladigan simmetrik shifrlash algoritmlari va raqamli imzo ishonchli bo'lsa, Shuningdek, raqamli imzo kalitlari to'g'ri autentifikatsiyalansa, bu protokollari nisbatan «o'rtadagi odam» hujumi ijobiy natija bermaydi.

Kamchilik sifatida abonentlar autentifikasiyasining va kalitni qabul qilganligini tasdig'ining yo'qligini ko'rsatish mumkin. Bundan tashqari ushbu protokol «o'rtadagi odam» hujumiga nisbatan zaif.

Faraz qilaylik, M (buzg'unchi) A va B abonentlar o'rtasidagi xabarlarni tutib olish hamda biridan ikkinchisiga boradigan xabarlarni blokirovka qilish imkoniga ega bo'lsin. Agar A va B abonentlar seans kaliti K ni uzatishda Shamir protokolidan foydalanishsa, u holda M nafaqat kalitni qiymatini bilishi, balki B abonentga yolg'on K_1 kalitni tiqishtirishi mumkin. Buning uchun u A abonentga o'zini B abonent sifatida tutishi va K kalitni olishi lozim. Undan so'ng B abonentga o'zini A abonent sifatida tutishi va unga K_1 kalitni tiqishtirishi kerak bo'ladi. Ushbu ishlarni bajargandan so'ng M (buzg'unchi) A abonentdan B abonentga jo'natiluvchi, K kalit bilan shifrlangan barcha xabarlarni o'qishi va unga o'zgartirish kiritib, K_1 kalit bilan shifrlab, B abonentga jo'natishi mumkin. Xuddi shu ishlarni B abonentdan A abonentga jo'natiladigan xabarlarga nisbatan bajaradi.

Izoh: «o'rtadagi odam» hujumiga nisbatan qarshi turish uchun ushbu protokolga o'zgartirish kiritish lozim. Buning uchun har abonent o'zlarining har bir xabarlariga elektron imzo qo'yishlari lozim bo'ladi. Ushbu holatda abonentlarning autentifikasiyasi masalasi hal qilinadi va buzg'unchi o'zini protokol ishtirokchisi qilib ko'rsatish imkonidan mahrum bo'ladi.

§7.15. Diffi-Xellman protokoli

Ushbu protokol umumiy maxfiy kalitni hosil qilish uchun ishlatiladi. Protokolning bardoshligi diskret logarifmlash masalasining murakkabligi bilan xarakterlanadi.

Protokolning parametrlari:

p – katta tub son;

$\alpha \in Z_p^*$ multiplikiv guruh elementi.

Protokolni amalga oshirish quyidagi qadamlarga asoslangan:

1. $A \rightarrow B: \alpha^x \bmod p$ (bu yerda x – tasodifiy maxfiy son);

2. $B \rightarrow A: \alpha^y \bmod p$ (bu yerda y – tasodifiy maxfiy son);

R_Y – Y abonent tomonidan tanlab olingan tasodifiy son;
 $data_Y$ – Y abonent tomonidan xabarga kiritilgan maxfiy ma'lumotlar,
ushbu parameter shart bo'lmagan parameterlar toifasiga tegishli.

k_Y – Y abonentning qisman kaliti;

Id_Y – Y abonentning identifikatori.

1. $A \rightarrow B: sert_A, M_A = (T_A, R_A, Id_A, data_A, P_B(k_A)), S_A(M_A);$

2. $B \rightarrow A: sert_B, M_B = (T_B, R_B, Id_B, R_A, data_B, P_A(k_B)), S_B(M_B);$

3. $A \rightarrow B: R_B, Id_B, S_A(R_B, Id_B).$

k_A, k_B qisman kalitlardan abonentlar oldindan kelishib olingan algoritm asosida umumiy seans kaliti K ni hosil qilishadi.

Ushbu protokolda A va B abonentlarning ochiq kalitlarini oldindan autentifikatsiya qilishga asoslangan.

Protokol nafaqat qisman kalitlarni abonentlar bir-birlariga uzatishga, balki raqamli imzodan foydalanib, ular bir-birlarini o'zaro autentifikatsiyalashga ham mo'ljallangan.

Protokolning 3-qadamida A abonent B abonentdan xabar olganligini imzolangan xabarni B abonentga jo'natish orqali tasdiqlaydi. Xabarlardan takroran foydalanishga asoslangan hujumlarni bartaraf qilish hamda aloqa kanalini blokirovka qilish va qalbaki xabarlarni jo'natilishini oldini olish uchun vaqt nishonidan foydalanilgan.

§7.16. Nidxem-Srederning transport protokoli

Ushbu protokolda ikkikalitli, ya'ni ochiq kalitli shifrlash algoritmi va quyida keltirilgan belgilashlardan foydalaniladi:

$P_Y(X)$ – X xabarni abonentning ochiq kaliti Y bilan shifrlash;

k_Y – Y abonentning qisman kaliti;

Id_A – A abonentning identifikatori (nomi).

Protokolni amalga oshirish quyidagi qadamlarga asoslangan:

1. $A \rightarrow B: P_B(k_A, Id_A)$;

2. $B \rightarrow A: P_A(k_A, k_B)$;

3. $A \rightarrow B: P_B(k_B)$.

k_A , k_B qisman kalitlardan abonentlar oldindan kelishib olingan algoritm asosida umumiy seans kaliti K ni masalan, $K = k_A \oplus k_B$ ko'rinishda hosil qilishadi.

Ushbu protokol A va B abonentlarning ochiq kalitlarini oldindan autentifikatsiya qilishga asoslangan. Shu sababli protokolning 2-3 qadamlari abonentlarning o'zaro autentifikatsiyalash va qisman kalitlarni olinganligini tasdiqlash vazifasini bajaradi. A abonent qabul qilgan qisman kaliti k_A 1-qadamda o'zi jo'natgan qisman kalit bilan mosligini 2-qadamda tekshirib ko'rishi lozim. Xuddi shu ishni 3-qadamda B abonent bajarishi kerak.

§7.17. X-509 standarti

X-509 standartiga ko'ra kalitlarni tarqatish protokolida quyidagi belgilashlar ishlatilgan:

$S_Y(X)$ – X xabar ostiga qo'yilgan Y abonentning raqamli imzosi;

$sert_Y$ – raqamli imzoning kalitini tekshirishda foydalaniladigan Y abonentning sertifikat;

$P_Y(X)$ – X xabarni Y abonentning ochiq kaliti bilan shifrlash (ochiq kalitli algoritm asosida);

T_Y – joriy xabarni shakllantirish vaqtida Y abonent tomonidan yaratilgan vaqt nishoni (belgisi);

jumladan, O'zbekiston Respublikasi ham o'zining O'zDSt 1092:2009 elektron raqamli imzo standartiga ega.

ERI imzolovchini identifikasiyalash va imzolangan hujjatni o'zgartirilmaganligini kafolatlashni tasdiqlovchi qandaydir axborotni imzolananayotgan axborotga qo'shish usulidir.

ERIlar telekommunikasiya kanallari orqali uzatiladigan elektron hujjatlarni aslligini - haqiqiyiligini ta'minlash uchun ishlatiladi. Ular qog'ozdagi odatdagi imzolarga qo'yiladigan barcha talablarni qanoatlantirishi zarur. Shu bilan bir vaqtda ularning fayl ko'rinishida taqdim qilinishi ERIlarga nisbatan yangi talablarni paydo bo'lishiga olib keidi. ERIlarni odatdagi imzolardan asosiy farqi ularni imzolananayotgan elektron hujjatga bog'liqligidadir.

ERI quyida keltirilgan asosiy xususiyatlarga ega bo'lishi lozim:

➤ Tekshirish, ya'ni axborot tizimidagi ixtiyoriy foydalanuvchi imzoni tekshirish imkoniyatiga ega bo'lishi;

➤ Rad etishni oldini olish, ya'ni hujjatni taqdim qilgan, imzolagan shaxsning aynan o'zi hujjatga imzo qo'yganligini tekshirish (shu jumladan, yuridik jihatdan tekshirish) imkoniyatini mavjud bo'lishi;

➤ Qalbakilashtirishni oldini olish, ya'ni bir shaxsni imzosini boshqa shaxs yaratish imkoninini mavjud bo'lmasligi;

➤ Imzolangan hujjatning ajralmas qismi bo'lishi, ya'ni ERIni butunlay boshqa hujjatga ko'chirish imkonini mavjud bo'lmasligi;

➤ Hujjatni butunligini himoyalashni ta'minlashi, ya'ni hujjatning mazmunini o'zgartirish yoki almashtirish imkonini mavjud emasligi.

Yuqorida keltirilgan xususiyatlariga ko'ra ERI quyidagi 4 ta masalani hal qilish uchun amaliyotda qo'llaniladi:

❖ Imzolangan hujjat haqiqatan ham imzo qo'ygan shaxs tomonidan jo'natilganligini tasdiqlash;

❖ Hujjatni imzolagan shaxsni o'z imzosini rad etishiga yo'l qo'ymaslik;

❖ Imzolangan hujjatni o'zgartirilmaganligini (butunligini) ta'minlash.

Elektron hujjatlarni imzolashning hozirgi kunda 3 ta turi mavjud:

1. Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash;

8-BOB. ELEKTRON RAQAMLI IMZO PROTOKOLLARI

Elektron raqamli imzo (ERI) paydo bo'lishining dastlabki yillaridayoq u AQSH va sobiq SSSR davlatlari o'rtasidagi yadro qurollarini sinash bo'yicha tuzilgan shartnoma shartlarini bajarilishini nazorat qilishda qo'llanilgan. Bu ikki davlat birining hududida boshqasi yadro qurollarini sinashini kuzatishi uchun seismograf joylashtirishi to'g'risida kelishib olishgan. Asosiy muammo bu davlatlarning har biri boshqasi tomonidan o'rnatilgan seismograf natijalarining qalbakilashtirilmasligiga ishonch hosil qilishlarida edi. Shuningdek, bir vaqtning o'zida har ikki tomon seismograf datchiklari yadro sinovlarini kuzatishi uchun aynan kerakli axborotlarni yuborayotganiga ishonch hosil qilishlari lozim edi. Raqamli imzoni qo'llanilishi ushbu ikki muammoni ham hal qildi: hududida seismograf joylashgan davlat uni natijalarini o'qishi mumkin, ammo seismograf natijalarini o'zgartirolmaydi, chunki kuzatuvchi ikkinchi davlat ma'lumotlar qalbakilashtirilganligini bilib qolishi mumkin edi.

Ushbu bobda elektron raqamli imzo protokollariga tegishli ma'lumotlar keltirilgan. Shuningdek, simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli hamda ochiq kalitli kriptotizimlardan foydalanib, hujjatlarni imzolash masalalari bayon etilgan. Elektron raqamli imzo imzo standartlarida qo'llaniladigan maxsus algoritmlar – DSA, GOST R 34.10-94 va GOST R 34.10-2001 elektron raqamli imzo algoritmlari keltirilgan.

§8.1. Elektron raqamli imzo

Ochiq kalitli kriptografiyaning paydo bo'lishi hamda uning kompyuter va axborot texnologiyalarida keng qo'llanilishi natijasida avvallari yechish mumkin bo'lmagan ko'pgina masalalarni yechish va ularni amaliyotga qo'llash imkoniyati paydo bo'ldi. Elektron raqamli imzo hozirgi kunda ochiq kalitli kriptografiyaning eng muhim elementlaridan biri bo'lib qolmoqda. Ilm fani rivojlangan ko'pchilik davlatlar, shu

(2) Smit Alisaning K_A maxfiy kalitini bilgani uchun qabul qilingan, shifrlangan xabarni K_A kalit bilan dastlabki matnga o'giradi.

(3) Smit xabarni Alisadan olganligi haqidagi tasdiqni dastlabki matnga o'girilgan xabarga qo'shadi va hosil bo'lgan yangi xabarni Bobning K_B kaliti bilan shifrlaydi.

(4) Smit shifrlangan xabarni Bobga jo'natadi.

(5) Xabarni qabul qilgan Bob o'zining K_B kaliti bilan dastlabki matnga o'giradi. Natijada Bob Alisaning xabarini hamda ushbu xabar Alisadan olinganligini tasdiqlaydigan Smitning xabarini o'qishi mumkin bo'ladi.

Ushbu usulda imzolash qog'ozdagi imzolashga ekvivalentmi hamda unda raqamli imzolar ega bo'lishi lozim bo'lgan xususiyatlar mavjudmi degan savollarga javob berish uchun quyidagi mulohazalardan foydalanish mumkin.

1. Bu imzo ishonchli. Chunki, Smit ishonchga loyiq bo'lgan, xolis shaxs va u xabar Alisadan kelganligini biladi. Xabar Alisadan jo'natilganligi haqidagi Smitni tasdig'i Bob uchun isbot vazifasini bajaradi.

2. Bu imzo qalbaki emas. Faqat Alisa (shuningdek, Smit ham maxfiy kalitni biladi, ammo Smit hamma ishonadigan ishonchli shaxs) K_A maxfiy kalitni biladi. Shu sababli faqat Alisa K_A maxfiy kalit bilan shifrlangan xabarni Smitga jo'natishi mumkin. Agar kimdir Alisani nomidan xabarni imzolamoqchi bo'lsa, Smit uni (2)-chi qadamda payqagan va xabarni haqiqiyiligini tasdiqlamagan bo'lar edi.

3. Ushbu imzoni takroran ishlatib bo'lmaydi. Agar Bob Smitni tasdig'ini olib, uni boshqa xabarga qo'shmoqchi bo'lsa, Smit undan xabarni va Alisaning shifrlangan xabarini taqdim qilishini so'raydi. Xabarni qabul qilgan Smit K_A kalit bilan uni shifrlab, Bob tomonidan taqdim qilingan shifrlangan xabar bilan bir xil emasligini payqagan bo'lar edi. Ushbu holatda Bob K_A kalitni bilmasligi sababli haqiqatan ham to'g'ri shifrlangan xabarni hosil qilolmaydi.

4. Imzolangan hujjatni o'zgartirish mumkin emas. Hujjatni qabul qilgan Bob uni o'zgartirishga harakat qilsa, yuqorida bayon qilingan usulda Smit uning tovlamachiligini payqagan bo'lar edi.

2. Asimmetrik kriptotizimlar asosida hujjatlarni imzolash;
3. Maxsus algoritmlar, ya'ni ERI protokollari asosida hujjatlarni imzolash.

Axborotni uzatishda jo'natuvchining maxfiy kalitidan va axborotni qabul qilishda axborot jo'natuvchining ochiq kalitidan foydalanishga asoslangan qandaydir ERIni hisoblashdan foydalanuvchi protokollar *ERI protokollari deyiladi*.

Maxsus elektron raqamli imzo algoritmlarida ERIdan foydalanish 2 bosqichdan iborat:

1. Raqamli imzoni shaklantirish;
2. Raqamli imzoni tekshirish.

Raqamli imzoni shaklantirish bosqichida xabarni jo'natuvchining maxfiy (yopiq) kalitidan foydalaniladi.

Raqamli imzoni tekshirishda esa kalitni taqsimlash markazida yaratiladigan va haqiqiyliги ushbu markaz tomonidan tasdiqlanadigan, imzo kaliti sertifikatı shaklida taqdim qilingan jo'natuvchining ochiq kalitidan foydalaniladi.

§8.2. Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli

Faraz qilaylik, Alisa xabarni imzolab, uni Bobga jo'natishni rejalashtirdi. U bu ishni simmetrik kriptotizim va uchinchi shaxs - Smit ishtirokidan foydalanib, amalga oshirishi mumkin. Smit imzoni amalga oshirishda zarur bo'ladigan barcha vakolatga ega bo'lgan xolis shaxs. Unga Alisa ham Bob ham birdek ishonadi.

Protokolni amalga oshirishdan oldin Smit Alisa va Bobga mos holda K_A va K_B maxfiy kalitlarni tarqatadi. Bu kalitlar ko'pgina hujjatlarni imzolashda ko'p marta ishlatilishi mumkin.

Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli quyida keltirilgan protokol qadamlari asosida amalga oshiriladi.

- (1) Alisa K_A maxfiy kaliti yordamida xabarni shifrlab, Smitga jo'natadi.

Boshqa ochiq kalitli kriptografik algoritmlarda, masalan, DSAda raqamli imzo uchun alohida algoritm ishlatiladi va bu algoritmdan shifrlashda foydalanilmaydi.

Ochiq kalitli kriptografiyadan foydalanib, hujjatlarni imzolashda foydalaniladigan kriptografik protokol quyidagi qadamlarni amalga oshirishga asoslangan bo'ladi:

(1) Xabarni jo'natuvchi shaxs o'zining maxfiy kalitidan foydalanib, hujjatni shifrlaydi. Shunday qilib u hujjatni imzolaydi.

(2) Xabarni jo'natuvchi shaxs imzolangan hujjatni qabul qiluvchiga jo'natadi.

(3) Qabul qiluvchi xabarni jo'natuvchi shaxsning ochiq kalitidan foydalanib, hujjatni dastlabki matnga o'giradi. Shu tarzda u imzoni tekshiradi.

Ushbu protokol oldingisiga nisbatan ancha yaxshi. Uchinchi shaxs – Smit hujjatni imzolashda ham, uni tekshirishda ham ishtirok etmaydi (u faqatgina xabarni jo'natuvchi shaxsning ochiq kalitini tasdiqlash uchun kerak). Smit, hattoki bahsni yechish uchun kerak ham emas: Qabul qiluvchi (3)-chi qadamni amalga oshira olmasa, u holda imzo qalbaki ekanligini anglaydi. Bunday imzo quyida keltirilgan barcha talablarga mos keladi:

1. Ushbu imzo ishonchli. Qabul qiluvchi xabarni jo'natuvchi shaxsning ochiq kalitidan foydalanib, xabarni dastlabki matnga o'giringanda bu xabarni haqiqatan ham xabarni jo'natuvchi shaxsning o'zi imzolaganligiga ishonch hosil qiladi.

2. Ushbu imzo qalbaki emas. Faqatgina xabarni jo'natuvchi shaxs maxfiy kalitni biladi.

3. Ushbu imzodan takroran foydalanish mumkin emas. Imzo hujjatning ajralmas qismi bo'lib, uni boshqa hujjatga ko'chirish mumkin emas.

4. Imzolangan hujjatni o'zgartirish mumkin emas. Hujjat ixtiyoriy o'zgarishdan so'ng xabarni jo'natuvchi shaxsning ochiq kalitidan foydalanib, tasdiqlanish (imzoni tekshirish) imkoniyatini yo'qotadi.

5. Imzoni rad qilib bo'lmaydi. Qabul qiluvchi tomonidan imzoni tekshirishda xabarni jo'natuvchi shaxsning ishtiroki yoki yordami talab qilinmaydi.

5. Imzoni rad qilish mumkin emas. Agar Alisa hech qachon xabar jo'natmaganligini e'lon qilsa, Smitni tasdig'i uning teskarisini isbotlaydi. Smitga barcha ishonishi va uning barcha aytganlari rost ekanligiga bu yerda yana bir marta e'tibor qaratish lozim.

Simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokoli amalda ishlaydi, ammo uchinchi shaxs – Smitdan katta vaqt sarflashini talab qiladi. U kun bo'yi shifrlangan xabarlarni dastlabki matnga o'girishi va uni tasdig'i bilan qaytadan shifrlashi lozim bo'ladi. Shuningdek, Smit xabarlarni ma'lumotlar bazasida saqlashi lozim bo'ladi. Imzolangan hujjatlar asosida xabar alamashinuvchi juftliklar bir necha bo'lishi faraz qilinsa, Smitning ish hajmi va unga sarflaydigan vaqti haqida tassavurga ega bo'lish mumkin. Ya'ni, bu yerda Smit yoki uning vazifasini bajaruvchi qandaydir kompyuter dasturi bu aloqa tizimida muhim tugun nuqtasi sifatida xizmat qiladi.

Barchani ishonchiga loyiq bo'lgan, Smitga o'xshagan xolis shaxsni topish amalda mushkul masala hisoblanadi. Agar million imzolardan qandaydir biriga u xato qilsa, hech kim unga ishonmay qo'yadi. Yoki bo'lmasa uning maxfiy kalitlar saqlanadigan ma'lumotlar bazasini kimdir qandaydir yo'llar bilan qo'lga kiritsa-chi?

Yuqorida keltirilgan mulohazalarga asoslanib, bayon etilgan simmetrik kriptotizim va uchinchi shaxs ishtirokidan foydalanib, hujjatlarni imzolash protokolidan amalda foydalanish bir qator kamchiliklar sababli murakkab masala ekanligiga ishonch hosil qilish mumkin.

§8.3. Ochiq kalitli kriptografiyadan foydalanib, hujjatlarni imzolash

Hozirgi kunda raqamli imzolardan foydalanuvchi ochiq kalitli kriptografik algoritmlar amaliyotda keng qo'llanilmoqda. Ushbu algoritmlarning ayrimlarida, masalan, RSA kriptotizimida qabul qiluvchining ochiq kaliti shifrlash, maxfiy (yopiq) kaliti esa dastlabki matnga o'girish uchun ishlatiladi. ERIda esa xabar jo'natuvchi o'zining maxfiy kalitidan foydalanib, hujjatni imzolab, ishonchli raqamli imzoga ega bo'lishi mumkin.

Bir yo'nalishli xesh funksiyalarga asoslangan raqamli imzo protokollaridan foydalanishning bir qator foydali tomonlari bor. Masalan, imzo hujjatdan ajratilgan holda, alohida bo'lishi mumkin. Ikkinchi tomondan qabul qiluvchining imzoni va hujjatni saqlovchi xotirasi hajmiga talab kamayadi. Arxiv tizimi ushbu holda hujjatni o'zini saqlamasdan, balki uni mavjudligini tasdiqlash uchun ushbu protokoldan foydalanadi. Markaziy ma'lumotlar bazasida ularning xesh qiymatlari saqlanishi mumkin. Bu ma'lumotlar esa kelgusida paydo bo'lishi mumkin bo'lgan o'zaro bahslarni hal qilishda muhim ahamiyatga ega.

Hozirgi kunda ochiq kalitli kriptotizimlarga asoslangan bir qancha raqamli imzo algoritmlari mavjud. Ushbu algoritmlarning har birida maxfiy (yopiq) kalit hujjatni imzolashda, ochiq kalit imzoni tekshirishda qo'llaniladi. Ayrim hollarda hujjatni imzolash jarayoni maxfiy kalit bilan shifrlash, imzoni tekshirish jarayoni esa ochiq kalit bilan dastlabki matnga o'girish deb nomlanadi. Bu holat ushbu algoritmlarning ayrimlari uchun, masalan, RSA uchun o'rinli bo'lib, boshqa algoritmlar uchun chalg'itishi mumkin. Masalan, bir yo'nalishli xesh funksiya va vaqt belgilaridan foydalanish imzolashda va uni tekshirishda qo'shimcha ish bosqichlarini paydo bo'lishiga olib keladi.

Ko'pgina kriptografik algoritmlardan elektron raqamli imzolarda foydalanish mumkin, ammo ulardan shifrlashda foydalanish mumkin emas.

§8.4. Maxsus algoritmlar, ya'ni ERI protokollari asosida hujjatlarni imzolash

DSA elektron raqamli imzo algoritmi

1991 yil avgust oyida Amerikaning Standartlar va texnologiyalar milliy instituti (NIST) tomonidan o'zining DSS (Digital Signature Standard) raqamli imzo standartida elektron raqamli imzo algoritmi DSA (Digital Signature Algorithm) dan foydalanish taklif qilindi. Ushbu standartda ochiq kalitdan foydalanuvchi DSA elektron raqamli imzo algoritmi keltirilgan.

DSS raqamli imzo standartida ochiq kalitdan xabarni qabul qiluvchi shaxs ma'lumotlarning butunligini va jo'natuvchining shaxsini aniqlashda

Ma'lum bir shartlarda qabul qiluvchi tavlamachilik qilishi mumkin. U hujjatni imzo bilan birgalikda takroran ishlatishi mumkin.

Faraz qilaylik, Alisa qiymati 1000000 so'm bo'lgan chekni imzolab, uni Bobga jo'natdi. Bob chekni bankka topshirdi. Bank imzoni tekshirib, pulni bir hisob raqamidan boshqasiga o'tkazadi.

Bob tavlamachilik qilish maqsadida elektron chekni bir nusxasini o'zida saqlab qoladi. Keyingi haftada u chekni shu yoki boshqa bankga olib boradi va bank imzoni tekshirib, pulni bir hisob raqamidan boshqasiga o'tkazadi. Agar Alisa o'zining chek daftarini tekshirib turmasa, Bob tavlamachiligini yil davomida yoki bir necha marta amalga oshirishi mumkin.

Yuqoridagi sabablarga ko'ra raqamli imzolar ko'p hollarda vaqt belgisidan ham tashkil topadi. Hujjatni imzolash sanasi va vaqti hujjatga qo'shiladi va hujjatning barcha mazmuni bilan birgalikda imzolanadi. Bank esa ma'lumotlar bazasida ushbu vaqt belgisini saqlaydi. Endi Bob ikkinchi marta imzolangan chekni bankga taqdim qilganida, bank o'zining ma'lumotlar bazasidan vaqt belgisini tekshiradi. Shu sababli ushbu holda Bob tavlamachilik qilishiga yo'l qo'yilmaydi.

Amaliyotda ko'pchilik hollarda ochiq kalitli kriptografik algoritmlar katta hajmdagi hujjatlarni imzolashda yetarlicha samara bermaydi. Vaqtdan yutish maqsadida raqamli imzo protokollari, ayrim hollarda bir yo'nalishli xesh funksiyalardan foydalaniladi. Ushbu holda Alisa hujjatni emas, balki uning xesh qiymatini imzolaydi. Bunday turdagi protokollar quyidagi tarzda amalga oshiriladi:

(1) Alisa hujjatning xesh qiymatini hisoblaydi.

(2) Alisa o'zining maxfiy kalitidan foydalanib, hujjatni xesh qiymatini shifrlaydi. Shunday qilib u hujjatni imzolaydi.

(3) Alisa hujjatni va imzolangan xesh qiymatni Bobga jo'natadi.

(4) Bob Alisa jo'natgan hujjatning xesh qiymatini qabul qiladi. Undan so'ng raqamli imzo algoritmi va Alisaning ochiq kalitidan foydalanib, hujjatni imzolangan xesh qiymatini dastlabki matnga o'giradi. Hujjatni imzolangan xesh qiymati u tomonidan hisoblangan xesh qiymati bilan bir xil bo'lsa, imzoni to'g'ri deb hisoblaydi.

Bunday holatlarda protokolda ishlatiladigan bir yo'nalishli xesh funksiyalar va raqamli imzo algoritmlari haqida oldindan kelishib olinadi.

r va s parametrlar juftligi (r,s) jo'natuvchining imzosi hisoblanadi. Jo'natuvchi ushbu (r,s) imzoni m xabar bilan birga qabul qiluvchiga jo'natadi.

Imzoni tekshirish:

Qabul qiluvchi quyidagi hisoblashlarni bajarish natijasida imzoni tekshiradi.

1. $w = s^{-1} \bmod q$ parametrni va $h(m)$ xesh qiymatni hisoblaydi.

2. $u_1 = h(m)w \bmod q$ va $u_2 = (rw) \bmod q$ parametrlar qiymatlarini hisoblaydi.

3. y ochiq kalitdan foydalanib, $v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q$ ni hisoblaydi.

4. Arap $v \Rightarrow$ bo'lsa, M hujjatni (r,s) imzosini haqiqiy deb hisoblaydi.

r va s parametrlarning har biri q sonidan kichik bo'lganligi bois, DSA asosidagi imzo uzunligi 320 bit bo'ladi. Ushbu imzoning xavfsizligi diskret logarifmlash masalasining murakkabligiga asoslanadi.

GOST R 34.10-94 elektron raqamli imzo standarti

GOST R 34.10-94 standarti 1994 yilda Rossiyaning elektron raqamli imzo standarti sifatida tasdiqlangan. Ushbu standart El-Gamal ERI algoritmiga asoslangan. Shu bois, GOST R 34.10-94 ERI standarti tashqi ko'rinishidan DSSga o'xshab ketadi.

GOST R 34.10-94 standarti GOST 12847-89 simmetrik blokli shifrlash algoritmidan foydalanuvchi, GOST R 34.11-94 xeshlash standartiga mos keluvchi h xeshlash funksiyasidan foydalanishga mo'ljallangan.

ERI kalitlarini generatsiya qilish. Xabarni jo'natuvchisi quyidagi parametrlarni generatsiya qiladi:

p – uzunligi 509 bitdan 512 bitgacha yoki 1020 bitdan 1024 bitgacha bo'lgan katta tub soni;

q – $(p-1)$ soninig bo'luvchisi bo'lib, uzunligi 254 bitdan 256 bitgacha tub soni;

a – $(p-1)$ sonidan kichik bo'lib, unung uchun $a^q \bmod p = 1$ munosabat o'rinli bo'lishi lozom;

foydalanadi. Shuningdek, imzoning to'g'riligini va unga bog'liq ma'lumotlarni tekshirishda uchinchi shaxs tomonidan ushbu standart foydalanishi mumkin.

DSA Shnor va El-Gamal elektron raqamli imzo algoritmlari asosida hosil qilingan. DSA elektron raqamli imzo algoritmidagi elektron hujjatni jo'natuvchi va qabul qiluvchi hisoblashlarda quyidagi katta butun sonlardan foydalanadilar:

$p - L$ bit uzunlikdagi tub son. Bu yerda L 512 dan 1024 gacha oraliqdagi, bitlar uzunligi 64 ga karrali bo'lgan qiymatni qabul qiladi. $q - 160$ bitli, $p-1$ ni bo'luvchisi bo'lgan tub son. g soni natural son bo'lib, bu son quyidagi munosabatdan aniqlanadi:

$$g = h^{(p-1)/q} \bmod p.$$

Bu yerda $h - h^{(p-1)/q} \bmod p > 1$ tengsizlikni qanoatlantiruvchi, $p-1$ dan kichik bo'lgan ixtiyoriy son. x soni $-q$ tub sonidan kichik bo'lgan son. $H(m)$ - SHA-1 xeshlash algoritmidan foydalunuvchi, bir tomonlama xesh-funksiya.

y ochiq kalit quyidagi munosabat asosida aniqlanadi:

$$y = g^x \bmod p.$$

Keltirilgan parametrlardan 3 ta parametr $- p, q$ va g parametrlar ochiq kalit hisoblanadi, ya'ni ushbu parametrlar maxfiy bo'lmagan parametrlardir. Ular tarmoqdagi barcha foydalanuvchilar uchun umumiy bo'lishi ham mumkin. x soni elektron raqamli imzoni shakllantirishda jo'natuvchining yopiq (maxfiy) kaliti, y soni elektron raqamli imzoni tekshirishda jo'natuvchining ochiq kaliti vazifasini bajaradi.

m xabarni imzolash uchun quyidagi qadamlar asosidagi amallar bajariladi.

Imzolash:

- (1) Jo'natuvchi q dan kichik bo'lgan k tasodifiy sonini hosil qiladi.
- (2) Jo'natuvchi $r = (g^k \bmod p) \bmod q$ va $k^{-1} \bmod q$ ni hisoblaydi.
- (3) Jo'natuvchi $s = (k^{-1}(H(m) + xr)) \bmod q$ ni hisoblaydi.
- (4) Agar $s=0$ bo'lsa, 1-chi qadamga o'tiladi ($s=0$ bo'lsa, $s^{-1} \bmod q$ mavjud bo'lmaydi. Imzoni tekshirishda s dan foydalaniladi).

almashtirishlardan foydalanishga asoslangan. Standart ERIlarni shakllantirish va tekshirish jarayonlarini belgilaydi.

GOST R 34.10-2001 ERI standarti GOST R 34.10-94 standarti asosida yaratilgan bo'lib, unga nisbatan yuqori bardoshlilik darajasiga ega hisoblanadi.

GOST R 34.10-2001 algoritmining bardoshliliği elliptik egri chiziq nuqtalari guruhida bajariladigan diskret logarifmlash masalasining murakkabligiga va algoritmda foydalaniladigan xesh funksiyaning bardoshligiga asoslangan. Xesh-funksiya sifatida esa GOST R 34.11-94 standarti qo'llaniladi.

GOST R 34.10-2001 algoritmini qo'llash natijasida qiymati 512 bit uzunligidagi ikkilik ketma-ketligidan iborat raqamli imzo hosil qilinadi. Imzoni shakllantirishda elliptik egri chiziq moduli sifatida $p > 2^{255}$ sonidan foydalaniladi.

Kalitlarni generatsiya qilish:

Elliptik egri chiziq moduli sifatida foydalanuvchi $p > 2^{255}$ tengsizlikdan aniqlanadigan p tub soni tanlanadi.

$1 \leq a < p$ va $1 \leq b < p$ tengsizliklarni qanoatlantiruvchi

$$y^2 = x^3 + ax + b$$

E elliptik egri chiziqning a va b koeffitsientlari tanlanadi.

N elliptik egri chiziq nuqtalari guruhining tartib nomeri bo'lsin.

$qP = 0$ tenglik o'rinli bo'ladigan P nuqta tanlanadi. Shuningdek, q soni uchun quyidagi shartlar bajarilishi lozim:

$2^{254} < q < 2^{256}$ shartni qanoatlantiruvchi tub sonidir, $N = nq$, bu yerda $n \geq 1$.

$0 < d < q$ shartni qanoatlantiruvchi qandaydir d soni tanlanadi.

$Q = dP$ nuqta hisoblanadi.

Imzoning ochiq kaliti: a, b, p, P, q, Q .

Imzoning maxfiy kaliti: d .

Xabarni imzolash. M xabar uchun ERI qiymatini hisoblash kerak bo'lsin. h – xeshlash funksiyasi bo'lsin.

$x - q$ sonidan kichik bo'lgan natural son, ushbu son xabarni jo'natuvchisining yopiq kaliti vazifasini bajaradi;

$y = a^x \bmod p$ – jo'natuvchisining ochiq kaliti vazifasini bajaradi

p, q va a parametrlar ochiq hisoblanadi va shu sababli tarmoqdagi barcha foydalanuvchilar uchun umumiy bo'lishi mumkin.

ERIni shakllantirish. Buning uchun xabarni jo'natuvchisi quyidagi ishlarni quyida keltirilgan tartibda amalga oshiradi:

1. Jo'natilishi lozim bo'lgan m xabarni 256 bitli $h=h(m)$ xesh qiymati GOST R 34.11-94 xeshlash standarti asosida hisoblanadi.

2. q sonidan kichik bo'lgan k natural soni tanlanadi.

3. $w = a^k \bmod p$ va $w' = w \bmod q$ parametrlarni qiymati hisoblanadi (standartga ko'ra w' ning qiymati 256 bit bo'lishi belgilangan). Agar $w'=0$ bo'lsa, 2-chi qadamga qaytib, k natural sonining qiymati qayta tanlanadi.

4. $s = (xw' + kh) \bmod q$ parametрни qiymati hisoblanadi (standartga ko'ra s ning qiymati 256 bit bo'lishi belgilangan). Agar $s=0$ bo'lsa, 2-chi qadamga qaytib, k natural sonining qiymati qayta tanlanadi.

(w', s) juftlik m xabarni imzosi hisoblanadi.

5. m xabar va unga mos keluvchi (w', s) imzo qabul qiluvchiga jo'natiladi.

ERIni tekshirish. Buning uchun xabarni qabul qiluvchi quyidagi ishlarni quyida keltirilgan tartibda amalga oshiradi:

1. Qabul qilingan m' xabarni xesh qiymati $h'=h(m')$ ni qayta hisoblaydi. Agar $m=m'$ bo'lsa, u holda $h = h'$ tenglik o'rinli bo'ladi.

2. $v = (h')^{q-2} \bmod q$ hisoblanadi,

3. $z_1 = (s \cdot v) \bmod q$ va $z_2 = ((q - w') \cdot v) \bmod q$ parametrlarni qiymati hisoblanadi.

4. $u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q$ parametрни qiymati hisoblanadi.

5. Agar $w'=u$ bo'lsa, u holda imzo haqiqiy va m xabar o'zgartirilmagan deb hisoblanadi.

GOST R 34.10-2001 elektron raqamli imzo standarti

Rossiyaning GOST R 34.10-2001 elektron raqamli imzo standarti ochiq kalitli kriptotizimlar sinfiga kiradi. Ushbu standart chekli maydonda aniqlangan elliptik egri chiziq nuqtalari guruhida bajariladigan kriptografik

Q nuqtaning qiymati hisoblanadi: $Q = dP$:

$(752, 453) \cdot 111 = (272, 824)$. Demak, $Q = (272, 824)$.

Xabarning imzosi. Imzolanishi lozim bo'lgan xabarning sonli ko'rinishi $M = 240$ bo'lsin.

Tasodifiy holda k soni tanlanadi: $k = 211$.

C nuqtaning qiymati hisoblanadi: $C = kP$:

$(752, 453) \cdot 211 = (787, 220)$. Demak, $C = (787, 220)$.

C nuqtaning x koordinatasi $x = 787$.

r sonini aniqlaymiz: $r = x \bmod q$, $r = 787 \bmod 521 = 266$.

s sonini aniqlaymiz: $s = (ek + dr) \bmod q$,

$s = (240 \cdot 211 + 111 \cdot 266) \bmod 521 = 453$, $s = 453$.

M xabarning imzosi: $(r = 266, s = 453)$.

Xabarni imzosini tekshirish. Kerakli parametrlarning qiymatlari hisoblanadi:

$v = e^{-1} \bmod q$, $v = \frac{1}{e} \bmod q = (1/240) \bmod 521 = 432$. $v = 432$.

$z_1 = sv \bmod q$, $z_1 = 453 \cdot 432 \bmod 521 = 321$. $z_1 = 321$.

$z_2 = -rv \bmod q$, $z_2 = ((0 - 266) \bmod 521 * 432) \bmod 521 = 229$. $z_2 = 229$.

$C = z_1P + z_2Q = (x_0, y_0) = (683, 384) + (864, 236) = (787, 220)$.

R ni qiymati hisoblanadi: $R = xc \bmod q$, $R = 787 \bmod 521 = 266$.

$R = 266 = r$. Demak, imzoni tekshirish muvaffaqiyatli yakunlandi. Imzo haqiqiy deb qabul qilinadi.

$e = h(M) \bmod q$ tenglikdan e soni aniqlanadi, agar $e = 0$ bo'lsa, $e = 1$ qilib tanlanadi.

$0 < k < q$ shartni qanoatlantiruvchi tasodifiy k soni tanlanadi.

Koordinatalari (x_c, y_c) bo'lgan $C = kP$ nuqta hisoblanadi.

Endi $r = x_c \bmod q$ tenglik o'rinli bo'ladigan r ning qiymati aniqlanadi. Agar $r = 0$ bo'lsa, k sonini qaytadan generasiya qilish va r ning yangi qiymatini aniqlash lozim bo'ladi.

$s = (rd + ke) \bmod q$ tenglik o'rinli bo'ladigan s ning qiymati aniqlanadi. Agar $s = 0$ bo'lsa, k sonini qaytadan generasiya qilish va s ning yangi qiymatini aniqlash lozim bo'ladi.

(r, s) sonlar juftligi M xabarga mos keluvchi ERI bo'ladi.

ERIni tekshirish:

$e = h(M) \bmod q$ tenglikdan e soni aniqlanadi, agar $e = 0$ bo'lsa, $e = 1$ qilib tanlanadi.

v soni shunday aniqlanadiki, natijada $v = e^{-1} \bmod q$ tenglik o'rinli bo'ladi.

z_1 va z_2 larning qiymatlari shunday aniqlanadiki, natijada $z_1 = sv \pmod{q}$, $z_2 = -rv \pmod{q}$ tengliklar o'rinli bo'ladi.

Elliptik egri chiziqning $C = z_1P + z_2Q$ tenglikni qanoatlantiruvchi $C(x_c, y_c)$ nuqtasi hisoblanadi.

$R = x_c \bmod q$ tenglikni qanoatlantiruvchi R ning qiymati hisoblanadi.

Agar $R = r$ tenglik bajarilsa, tekshirish muvaffaqiyatli yakunlanadi va imzo haqiqiy deb hisoblanadi. Aks holda imzo qabul qilinmaydi.

Misol. Ushbu misolda hisoblashlar murakkab bo'lmagani uchun unchalik katta bo'lmagan sonlar tanlangan. Shu sababli standartdagi ayrim shartlar soddalashtirilgan.

Parametrlarni generasiya qilish.

Elliptik egri chiziq moduli $p = 1021$.

Elliptik egri chiziq koeffitsientlari $a = 1$, $b = 1$.

Elliptik egri chiziqqa tegishli nuqta $P = (752, 453)$.

P nuqtaning rangi $q = 521$.

Tasodifiy holda $d = 111$ soni tanlanadi.

raqamlariga ega. Xaridor magazindan qandaydir tovarni sotib olishi uchun elektron to'lov tizimidagi quyida keltirilgan 3 ta asosiy tranzaksiyadan foydalaniladi:

1. xaridor bankdagi o'zining hisob raqamidan kerakli summani yechib oladi;

2. to'lov;

3. depozit.

Birinchi tranzaksiyada xaridor talab qilgan summasi uchun bank imzolagan elektron banknotni oladi. Bunda xaridorning hisob raqami talab qilingan summaga bank tomonidan kamarytiriladi.

To'lov tranzaksiyasida xaridor to'lov summasini ko'rsatgan holda elektron banknotni magazinga beradi. Magazin o'z navbatida bu axborotlarni bankka jo'natadi. Bank esa banknotning haqiqiylikini tekshirib ko'radi. Banknot haqiqiy bolsa, bank uning oldin bu banknot foydalanilganligi yoki aksini tekshirib ko'radi. Agar ushbu elektron banknot oldin foydalanilmagan bo'lsa, bank bu banknotni maxsus registrga kiritadi va xarid uchun mo'ljallangan summani magazin hisob raqamiga o'tkazadi. Bu haqda magazinni xabardor qiladi. Banknotdagi summa to'lov miqdoridan, y'ani magazindagi tovar narxidan yuqori bo'lsa, xaridorga (magazin orqali) qaytimni qaytaradi.

Deposit tranzaksiyasi vositasida xaridor to'lov tranzaksiyasidagi qaytimni bankdagi o'z hisob raqamiga qo'yishi mumkin.

Bankning xavfsizligi qalbaki elektron banknot yaratish uchun bankni imzosini qalbakilashirishning imkoni yo'qligi bilan izohlanadi.

Bizning maqsadimiz shunday elektron to'lov tizimini ishlab chiqishdan iboratki, ushbu to'lov sxemasi quyidagi xususiyatlarga ega bo'lsin:

- elektron qog'oz (banknot) bank hisob raqami bilan bog'lanmagan bo'lishi lozim;

- har bir elektron kupyura unikal nomerga ega bo'lib, bank tomonidan imzolangan bo'lishi lozim;

- mijozga berilgan elektron kupyuraning nomeri va kimga berilganligini bank bilmasligi kerak. Odatdagi naqd pullar bilan bo'ladigan to'lovlardagi kabi anonimlik saqlab qolinishi kerak.

9-BOB. ELEKTRON TO'LOVLAR XAVFSIZLIGINI TA'MINLASHDA KRIPTOGRAFIK PROTOKOLLARNI QO'LLASH

Hozirgi vaqtda Internetdan foydalanuvchi savdo tijorat bozorining yangi, tez o'suvchi sektoridir. Internet va Web qanaqadir tijorat amallarini oshirishga mo'ljallanmagan, shu sababli tarmoq bo'yicha yuboriladigan ma'lumotlar begonalar tomonidan tutib olinishi mumkin. Odatda elektron tijorat jarayonida ma'lumotlar matnlar ko'rinishida jo'natiladi, tutib olganlarga uni o'qish uchun hech qanday ortiqcha qiyinchiliklarni hojati qolmaydi. Shu sababli Internetda elektron to'lovlarni amalga oshirishda jo'natilayotgan axborotlarni, masalan, xarid kim tomonidan amalga oshirayotgani, qancha miqdordagi summaga xarid qilinayotganligi va shu kabi ma'lumotlarni begonalar tomonidan o'qilishi imkoniyatini yo'qotish, ya'ni elektron to'lovlar xavfsizligini ta'minlash axborot xavfsizligining hozirgi kundagi dolzarb muammolaridan biridir.

Elektron to'lovlar uchun birinchi kriptografik protokollar XX asrning 80-yillari boshida Shaum tomonidan taklif qilingan. Shu vaqtdan boshlab, ayniqsa oxirgi 10 yillikda elektron to'lovlar tizimida kriptografik protokollar keng qo'llanilmoqda. Bu holat rivojlangan mamlakatlar davlatlar organlari va banklarining elektron to'lov tizimlariga bo'lgan qiziqishlari bilan izohlanishi mumkin.

Ushbu bobda elektron to'lovlar xavfsizligini ta'minlashda kriptografik protokollarni qo'llash masalalari bayon etilgan. Zamonaviy elektron raqamli imzo (ERI) va ko'r-ko'rona imzolash protokollaridan foydalanib, elektron to'lovlar tizimini amalga oshirish masalalari muhokama qilingan. Mavzularni bayon qilishda protokol ishini murakkablashtirmaslik maqsadida ishtirokchilarni autentifikasiyalash va ular o'rtasidag xabarlarini butunligi masalalariga e'tibor qaratilmaydi.

§9.1. Elektron to'lovlar tizimining umumiy sxemasi

Ma'lumki, elektron to'lovlar tizimida uchta ishtirokchi qatnashadi: bank, xaridor va magazin. Xaridor va magazin bankda o'zlarining hisob

tekshiruv muvaffaqiyatli o'tsa, bank magazin hisob raqamiga 100\$ ni o'tkazadi. Bu haqda magazinni xabardor qiladi. Natijada magazin tovarni xaridorga sotadi.

Ushbu to'lov sxemasining kamchiligi anonimlikni yo'qligidadir. Bank xodimlari, xuddi Shuningdek, ochiq aloqa kanaliga aloqasi bo'lgan kimsalar, n soni qaysi xaridorga tegishli ekanligini eslab qolishlari va tovarni kim sotib olganligini aniqlashlari mumkin bo'ladi.

§9.3. Elektron to'lovlar xavfsizligining «ko'r-ko'rona» imzoga asoslangan sxemasi

Ikkinchi "yomon" to'lov sxemasini ko'rib chiqamiz. Bu sxema anonimlikni ta'minlaydi va "ko'r-ko'rona imzo"ga asoslangan.

Yana xaridor tovar sotib olmoqchi. U n sonini generasiya qiladi va hozircha uni bankga jo'natmay turadi. N soniga o'zaro tub bo'lgan tasodifiy r sonini generasiya qiladi va bankning ochiq kaliti d dan foydalanib,

$$\hat{n} = (n \cdot r^d) \bmod N$$

sonni hisoblaydi. Xaridor \hat{n} sonini bankga jo'natadi.

Bank

$$\hat{s} = \hat{n}^c \bmod N$$

sonini hisoblaydi va xaridorni hisob raqamidan 100\$ ni ushlab qolgan holda, xaridorga \hat{s} sonini jo'natadi.

Xaridor

$$r^{-1} \bmod N$$

sonini topadi va

$$s = (\hat{s} \cdot r^{-1}) \bmod N$$

ni hisoblaydi. Yuqoridagi formulalarga asosan xaridor quyidagi tenglikni hosil qilishi mumkin:

$$s = \hat{n}^c \cdot r^{-1} = (n \cdot r^d)^c \cdot r^{-1} = n^c r^{dc} \cdot r^{-1} = n^c r^1 \cdot r^{-1} = n^c \bmod N \quad (*)$$

Elektron qog'oz (banknot) to'lov tizimlarida foydalaniladigan, to'lovni amalga oshiruvchi shaxsni harakatlarini anonimligi va bankni xavfsizligini ta'minlash xususiyatiga ega bo'lgan vositadir.

§9.2. RSA raqamli imzodan foydalanib, elektron to'lovlar xavfsizligini ta'minlash

Birinchi "yomon" to'lov sxemasini bayon qilamiz. U RSA raqamli imzoga asoslangan. Bank quyidagi ma'lumotlarga ega bo'lsin: P, Q, c maxfiy sonlar va ochiq sonlar

$$N = PQ$$

$$d = c^{-1} \bmod (P-1)(Q-1)$$

Oldin bir xil nominaldagi, masalan, 100\$ lik kupyuradan foydalanishni ko'rib chiqish maqsadga muvofiq. Faraz qilaylik, 100\$ miqdoridagi summaga biror narsa xarid qilishni istaydi. Xaridor bankga elektron banknot nomerini anglatuvchi n sonini jo'natadi (buning uchun $[2, N-1]$ oraliqidagi tasodifiy son generatsiya qilinishi talab etiladi).

Bank

$$s = n^c \bmod N$$

sonini hisoblaydi va xaridorni hisobini 100\$ ga kamaytiradi. $\langle n, s \rangle$ banknotni shakllantirib, xaridorga jo'natadi. Parametr s bu bankni imzosi. Bankdan boshqa hech kim bu imzoni hosil qila olmaydi, chunki c soni maxfiy sonidir.

Xaridor tovarni sotib olish uchun $\langle n, s \rangle$ banknotni magazinga taqdim qiladi. Magazin tekshirish uchun ushbu banknotni bankga jo'natadi. Banknotni olishi bilan bank birinchi navbatda imzoni to'g'riligini tekshiradi (bankning ochiq kalitidan foydalanib, magazinni o'zi ham bu tekshiruvni bajarishi mumkin edi).

Odatda bank unga qaytarilgan barcha banknotlarni o'zida saqlaydi va shu sababli uning ro'yxatida n soni bor yoki yo'qligini tekshiradi. Agar n soni ro'yxatda bo'lsa, to'lov qabul qilinmaydi (kimdir banknotdan takroran foydalanmoqchi bo'layapti) va bu haqida magazinga xabar beradi. Agar

nomerlarini belgilashda 2 ta bir xil o'nlik sanoq tizimidagi sonlardan foydalanish qabul qilingan bo'lsin. Masalan, 22, 44, 55 va hakoza.

Xaridor bankdan banknot olish uchun yuqorida keltirilgan qoida asisida, masalan, $n=33$ ni tasodifiy tanladi. Endi u $N=119$ ga o'zaro tub bo'lgan, $r=67$ sonini tasodifiy tanlaydi. Undan so'ng xaridor

$$\tilde{n} = (33 \cdot 67^5) \bmod 119 = (33 \cdot 16) \bmod 119 = 52$$

ni hisoblaydi va aynan 52 sonini bankka jo'natadi.

52 sonini qabul qilgan bank xaridorni hisob raqamini 100\$ ga kamaytirib, ushbu summani bank hisobiga o'tkazadi va

$$\tilde{s} = 52^{77} \cdot \bmod 119 = 103$$

sonini hisoblab, xaridorga jo'natadi.

Xaridor $r^{-1} = 67^{-1} \bmod 119 = 16$ sonini hisoblaydi. Ushbu songa asosan

$$s = (\tilde{s} \cdot r^{-1}) \bmod N = (103 \cdot 16) \bmod 119 = 101$$

bankni imzosini hisoblab, to'lovga yaroqli banknot - $\langle n, s \rangle = \langle 33, 101 \rangle$ ni hosil qiladi. Bu banknotni tovar sitib olish uchun magazinga taqdim qiladi.

Magazin xaridordan olgan $\langle n, s \rangle = \langle 33, 101 \rangle$ banknotni bankka jo'natadi. Bank esa quyidagicha tekshiruv o'tkazadi:

✓ banknot nomeri $n=33$ haqiqatan ham qoida bo'yicha 2 ta bir xil o'nlik sanoq tizimidagi sonlardan tuzilganligini;

✓ oldin bu nomerdagi banknot bankka taqdim qilinmaganligini;

✓ bank imzosi haqiqiyiligini, ya'ni $33^5 \bmod 119 = 101$.

Ko'rinib turibdiki, barcha tekshiruvlar muvaffaqiyatli yakunlandi, Shu sababli bank magazin hisob raqamiga 100\$ ni o'tkazadi va bu haqida magazinga xabar qiladi. Magazin esa o'z navbatida xaridorga tovarni berib yuboradi.

ya'ni, n soniga mos keluvchi bankning imzosini hosil qildi. Ammo, n sonini o'zini na bank, na boshqa biron kimsa ko'rishga muvaffaq bo'lmadi. s sonini hisoblash "ko'r-ko'rona imzo" deb ataladi, chunki haqiqiy xabar (n) ni imzo qo'yuvchi ko'rgan emas va ko'rishi ham mumkin emas.

Shunday qilib, xaridor ixtiyorida n soni hech kimga ma'lum emas, (*) bilan hisoblanadigan bank imzosi s hech qachon ochiq aloqa kanali orqali uzatilmadi. Xaridor $\langle n, s \rangle$ banknotni shakllantirib, xuddi yuqoridagi birinchi "yomon" sxemadagidek harakat qilishi mumkin. Endi bu safar bu banknot kimga tegishli ekanligini hech kim bilmaydi, ya'ni u anonim bo'lib qoladi.

Xaridor tomonidan $\langle n, s \rangle$ banknot taqdim qilinganidan so'ng magazin va bankni harakati birinchi sxemada ko'rsatilganidan hech qanday farq qilmaydi.

Elektron to'lovni ushbu sxemasi nega yomon hisoblanadi? U quyidagi kamchiliklarga ega: agar hech bo'lmaganda 2 ta haqiqiy banknot ma'lum bo'lsa, ulardan qalbaki banknotni hosil qilish mumkin. U quyidagicha qilinadi. Aytaylik, buzg'unchi (u xaridor yoki magazin bo'lishi mumkin) 2 ta haqiqiy banknotlar $\langle n_1, s_1 \rangle$, $\langle n_2, s_2 \rangle$ ga ega bo'lsin. U holda u qalbaki $\langle n_3, s_3 \rangle$ banknotni osongina hosil qilish mumkin. Buning uchun u quyidagi sonlarni hisoblaydi:

$$n_3 = n_1 n_2 \bmod N,$$

$$s_3 = s_1 s_2 \bmod N.$$

Haqiqatan ham

$$n_3^c = (n_1 n_2)^c = n_1^c n_2^c = s_1 s_2 = s_3 \bmod N,$$

ya'ni, s_3 n_3 uchun to'g'ri imzodir va bankda uni qalbaki deb hisoblab, qabul qilmaslikka hech qanday asos yo'q (bank uni haqiqiysidan ajrata olmaydi). Bu esa RSA raqamli imzosining "multiplikativlik xossasi"dir.

Misol. Ushbu misolda bankning maxfiy parametrlari $P=17$, $Q=7$, $c=77$ va ularga mos keluvchi ochiq parametrlari $N=119$, $d=5$ bo'lsin. Banknotlarni qalbakilashtirishni oldini olish maqsadida ularning

Magazin va bankning qolgan barcha harakatlari oldingi ikkita to'lov sxemasida keltirilganidek bo'ladi.

Elektron pullar sxemasini realizatsiya qilishda hosil bo'ladigan ikkita muammoni hal qilishni ko'rib chiqamiz.

Taqdim qilingan to'lov sxemasida mustaqil, biri-biri bilan bog'liq bo'lmagan holda harakat qiluvchi xaridorlar yoki hattoki bitta xaridorni o'zi oldin ishlatgan banknotlari nomerlarini eslay olmasligi mumkin. Shu sababli tasodifan ikki yoki undan ortiq bir xil nomerli banknotlar generatsiya qilinishi mumkin. To'lov protokoli shartiga ko'ra ushbu banknotlardan faqat birini (qaysi biri oldin bankga taqdim etilsa) bank to'lov sifatida qabul qilishi mumkin. Bunday paytda protokolda foydalaniladigan sonlar o'lehovlarini e'tiborga olish lozim bo'ladi. Agar banknot nomeri uzunligi 512 bitdan iborat bo'lgan son bo'lib, xaridor haqiqatan ham uni tasodifan generatsiya qilgan bo'lsa, u holda ikkita bir xil nomerlarni hosil qilish ehtimoli juda kichik.

§9.5. Turli xil qiymatga ega bo'lgan banknotlar uchun elektron to'lov sxemasi

Elektron to'lovning ko'rib chiqilgan sxemalarida bir xil nominaldagi banknotlardan foydalanish o'rganiladi. Bu albatta xaridor uchun noqulay. Turli xil nominaldagi banknotlardan foydalanish muammosini quyidagicha hal qilish mumkin. Bank

$$d = c^{-1} \bmod (P-1)(Q-1)$$

tenglikni qanoatlantiruvchi (c, d) – yopiq va ochiq kalitlar juftliklarini ishlab chiqadi va masalan, d_1 1000 so'mga, d_2 500 so'mga va h.k. mos keladi deb e'lon qiladi. Xaridor bankdan "ko'r-ko'rona imzo" ni so'rashdan oldin u qanaqa nominaldagi banknotni olishni xohlayotganini qo'shimcha tarzda bankga xabar qiladi. Bank u xabar qilgan nominalga teng summani uning hisob raqamidan chiqarib tashlab, mos c , maxfiy sonda foydalanib, imzoni shakllantiradi. Imzolangan banknotni olgandan so'ng, bank o'z imzosini tekshirish uchun navbatma-navbat d_1, d_2 va h.k. ochiq kalitlardan foydalanadi. Agar banknotlarni parametri n uning

§9.4. Elektron to'lovlar xavfsizligining bir tomonlama funksiyaga asoslangan sxemasi

Endi bundan oldingi ikkita elektron to'lov sxemasidagi kachiliklardan xoli bo'lgan elektron to'lovlar xavfsizligining bir tomonlama funksiyaga asoslangan modelini ko'rib chiqamiz. Ushbu sxemada

$$f: \{1, \dots, N\} \rightarrow \{1, \dots, N\}$$

bir tomonlama funksiya (f ni hisoblash oson, lekin uning teskarisi f^{-1} ni hisoblash juda murakkab) dan foydalaniladi. f funksiya maxfiy emas, u barchaga (xaridorga ham, bankga ham va magazinga ham) ma'lum. Endi banknot $\langle n, s_f \rangle$ sonlar juftligi sifatida aniqlanadi, bu yerda s_f quyidagicha aniqlanadi:

$$s_f = (f(n))^e \bmod N.$$

ya'ni, n emas, balki $f(n)$ ni qiymati imzolanadi.

Xaridor hech kimga ko'rsatmasdan n ni generasiya qilib, $f(n)$ ni hisoblaydi va bankda "ko'r-ko'rona imzo" yordamida $f(n)$ sonini imzolaydi. Natijada $\langle n, s_f \rangle$ banknotni shakllantiradi. Ushbu banknot xuddi ikkinchi sxemadagi kabi barcha yaxshi xususiyatlarga ega bo'lib, f^{-1} ni hisoblash mumkin bo'lmaganligi sababli ushbu banknotni qalbakilashirish mumkin emas. Bu holda imzoni (ya'ni, banknotni haqiqiyligini) tekshirish uchun $f(n)$ ni hisoblash lozim bo'ladi va

$$s_f^d \bmod N = f(n)$$

ekanligiga ishonch hosil qilish kerak bo'ladi.

Shuni ham qayd qilish lozimki, bir tomonlama funksiyani tanlashda ehtiyot bo'lish lozim. Masalan, $f(n) = n^2 \bmod N$ funksiya aslida bir tomonlama funksiya bo'lsa-da, ammo ushbu to'lov protokoli uchun yaramaydi. Ushbu funksiya yordamida hosil qilingan banknot ikkinchi sxemada keltirilgan "multiplikativlik xossasi" ga ega. Odatda amaliyotda $f(n)$ funksiya sifatida kriptografik xesh-funksiyalardan foydalaniladi.

Bu paragrafda $(N, (f(N))^{1/h} \bmod n)$ sonlari juftligiga mos keluvchi bir xil S^* qiymatga ega va nomeri N bo'lgan elektron banknot ko'rib chiqiladi.

Xaridor bankdagi o'zining hisob raqamidan kerakli summani yechib olish tranzaksiyasi.

Ixtiyoriy tranzaksiyada ishtirokchilar o'zaro autentifikasiyalashdan o'tishadi. Mavzuni bayon qilishda protokoldagi autentifikasiyalash qadamlari keltirilmaydi. Shuningdek, quyidagi belgilashlar ishlatiladi: X – xaridor, M – magazin, B – bank.

Bu tranzaksiyada xaridor talab qilgan summasi uchun bank imzolagan elektron banknotni oladi. Bunda xaridorning hisob raqami talab qilingan summaga bank tomonidan kamarytiriladi. Ushbu tranzaksiyani quyidagu tartibda amalga oshirish mumkin:

1. X : tasodifiy $N \in Z_n$ sonini va $0 < r < n$ shart asosida r sonini tasodifiy tanlaydi;

$$2. X \rightarrow B: b = f(N)r^h \bmod n;$$

$$3. B \rightarrow X: y = b^{h^{-1}} \bmod n;$$

$$4. X: x = y \cdot r^{-1} \bmod n.$$

Bu amallar ketma-ketligi bajarilgandan so'ng xaridor bank tomonidan imzolangan (N, x) banknotga ega bo'ladi.

Haqiqatan ham,

$$\begin{aligned} x &\equiv yr^{-1} = b^{h^{-1}}r^{-1} \equiv (f(N)r^h)^{h^{-1}}r^{-1} \equiv \\ &\equiv (f(N))^{h^{-1}} \cdot r \cdot r^{-1} \equiv (f(N))^{h^{-1}} \pmod{n}. \end{aligned}$$

Ushbu x imzoda banknotning qiymati (ya'ni, bu yerda banknotning qiymati h orqali ifodalanmoqda) haqida ma'lumot bor, ammo uning nomeri N haqida ma'lumot yo'q. Bu esa xaridor tovar sotib olayotgan vaqtda anonimlikni saqlashda muhim o'rin egallaydi.

Misol. Banknotning maksimal qiymati 15 so'm bo'lsin. Bu sonning ikkilik ko'rinishdagi qiymati $S = 15 = (1111)_2$. Demak, $c_1 = c_2 = c_3 = c_4 = 1$ va $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11$. U holda

nominalini ko'rsatuvchi fiksirlangan axborotlardan tashkil topsa, imzoni tekshirish masalasi yengillashadi, ya'ni bank birdaniga kerakli d , kalitdan foydalanadi.

§9.6. Bir xil qiymatga ega bo'lgan elektron banknotlar uchun Shaum sxemasi

Ushbu protokol parametrlari sifatida bank tomonidan quyidagilar tanlanadi:

p, q, p^*, q^* - katta tub sonlari bo'lib, bankning maxfiy kalitlari hisoblanadi.

$n = p \cdot q$, $n^* = p^* \cdot q^*$ - RSA moduli sifatida shakllantiriluvchi bankning ochiq kalitlari bo'lib, ular foydalanuvchilar uchun e'lon qilinadi.

$f: Z_n \rightarrow Z_n$ akslantirish xossasiga ega bo'lgan bir tomonlama funksiya.

$(N, (f(N))^{1/h} \bmod n)$ sonlar juftligi - $N < n$ nomerli, qiymati S so'm bo'lgan banknotni ifodalasin. Bu yerda $h = \prod_{i=1}^k p_i^{e_i}$, $S = (e_k, e_{k-1}, \dots, e_1)$ - banknotning qiymati ikkilik ko'rinishidagi ifodasi, p_i - i -chi toq tub son.

Misol. Qiymati $S=12$ so'm bo'lgan banknotni o'rganamiz. Banknotning ikkilik ko'rinishdagi qiymati $S=12=(1100)_2$. Demak, $e_1=e_2=0$, $e_3=e_4=1$, $e_i=0$ va $p_1=3$, $p_2=5$, $p_3=7$, $p_4=11$.

$$h = 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^1 = 7 \cdot 11 = 77.$$

Bundan kelib chiqadiki, qiymati $S=12$ so'm va nomeri N bo'lgan elektron banknotga $(N, (f(N))^{1/77} \bmod n)$ sonlari juftligi mos keladi.

Shuni ham qayd qilish lozimki, faqatgina p, q maxfiy kalitlarni bilgan shaxs, ya'ni bank n modul bo'yicha $f(N)$ ni kasr darajaga ko'tarishi mumkin. Teskari amalni, ya'ni h darajaga ko'tarishni n ochiq kalitni bilgan ixtiyoriy odam amalga oshirishi mumkin. Shu sababli, n modul bo'yicha $f(N)$ ni $1/h$ darajaga ko'tarish amalda nomeri N bo'lgan elektron banknotni bank tomonidan imzolanishini anglatadi.

tekshirib ko'radi. Agar tekshirish natijasi ijobiy bo'lsa, N xaridori registrga kiritadi va magazinga tranzaksiyani tugatish haqida xabar jo'natadi, agar tekshirish natijasi ijobiy bo'lmasa, protokolni to'xtatadi.

5. $B \rightarrow M: c = z^{d^{-1}} \bmod n^*$ - qaytim;

6. $M \rightarrow X: c$.

Bu protokolni bajarilishi natijasida magazin qiymati s so'm bo'lgan (N, l) banknotni bankdan oladi. Haqiqatan ham, $l = x^d = (f(N))^{d \cdot s} \bmod n$, bu yerda dh^{-1} qiymati s so'm bo'lgan banknotga mos keladi.

Xaridor $(N^*, cr^{-1} \bmod n^*)$ kupyura korinishidagi qaytimni oladi:

$$cr^{-1} \equiv z^{d^{-1}} r^{-1} \equiv (f(N^*) \cdot r^d)^{d^{-1}} r^{-1} \equiv (f(N^*))^{d^{-1}} r r^{-1} \equiv (f(N^*))^{d^{-1}} \bmod n^*.$$

Misol. Bu misolda oldingi misoldagi qiymati 15 so'm bo'lgan banknotdan foydalaniladi. Shu sababli, $(N, (f(N))^{1/155} \bmod n)$ banknotga ega bo'lgan xaridor narxi 7 so'm bo'lgan tovarni sotib olishni istaydi. Bu holda qaytim $s = 8 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$ so'm. Bu qaytimga mos keluvchi parametr $d = 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^1 = 11$.

Xaridor magazin orqali l, z, s, n^* (yig'ib boriladigan banknotlarda ishlatiladigan modul) parametrlarni quyidagi qiymatlarini bankka jo'natadi: $l = (f(N)^{1/155})^{11} = f(N)^{1/15}$, $z = f(N^*) \cdot r^{11}$, $s = 8$, n^* .

Bank qiymatlarni qabul qilgach, tegishli tekshirishlarni o'tkazib, magazin orqali xaridorga quyidagi qaytim c ni qaytaradi:

$$c = z^{1/d} \bmod n^* = (f(N^*) \cdot r^{11})^{1/11} \bmod n^* = (f(N^*))^{1/11} \cdot r \bmod n^*.$$

Xaridor ushbu qaytimni olgach, undan niqobni yechib, qiymati 8 so'm bo'lgan $(N^*, f(N^*)^{1/11} \bmod n^*)$ banknotga ega bo'ladi va uni yig'ish uchun saqlab qayadi.

$$h = 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 3 \cdot 5 \cdot 7 \cdot 11 = 1155.$$

Xaridor banknotning nomeri N va tasodifiy r sonini tanlab, $b = f(N)^{1155} \bmod n$ sonini bankka jo'natadi. Bank bu sondan foydalanib, $b^{1155} = f(N)^{1155} r \bmod n$ sonni hisoblaydi va uni xaridorga jo'natadi. Xaridor qabul qilgan sonidan niqobni olib, qiymati 15 so'm bo'lgan $(N, (f(N))^{1155} \bmod n)$ banknotga ega bo'ladi.

To'lov tranzaksiyasi.

Faraz qilaylik, xaridor qiymati S^* bo'lgan (N, x) elektron banknotga ega. U magazindan narxi $s < S^*$ so'm bo'lgan tovarni sotib olishni istaydi. Bu holda xaridor magazinga qiymati S^* bo'lgan banknotni taqdim qiladi va magazindan qaytim (S^* so'mdan qolgan pul) ni olishi kerak. Ushbu ko'rinishdagi qaytimlar n modul bo'yicha emas, balki n^* modul bo'yicha imzolangan va alohida qiymatga ega bo'lgan banknotlar ko'rinishida to'planib boradi. Ulardan to'lovlarda deyarli foydalaninlmaydi. Ma'lum miqdordagi banknotlarni yig'ib, xaridor ularni bankka topshirishi mumkin. Buning natijasida bank topshirilgan banknotlarning qiymatiga teng bo'lgan summani xaridorni hisob raqamiga o'tkazadi.

Ushbu protokolda bank va xaridor to'g'ridan-to'g'ri bir-birlari bilan muloqat qilishmaydi. Shu sababli ular o'rtasida o'zaro autentifikasiyalash o'tkazilmaydi. Bu esa to'lov jarayonida xaridorni anonimligini saqlaydi. Protokolda faqat bank va magazin o'zaro autentifikasiyalashdan o'tishadi. Bu jarayon mavzuni bayon qilishda tushirib qoldirilgan. To'lov tranzaksiyasi protokoli quyidagi tarzda amalga oshiriladi:

1. $X: S^* - s = (e_k, e_{k-1}, \dots, e_1)_2$ ikkilik ko'rinishidagi qaytimni va $d = \prod_{i=1}^k p_i^{e_i}$ parametрни hisoblab, $N^* \in Z_n$ va $0 < r < 1$ tasodifiy sonlarni tanlaydi;

2. $X \rightarrow M: s, n^*, l = (f(N)^{1/h})^d \bmod n, z = f(N^*) \cdot r^d \bmod n^*$;

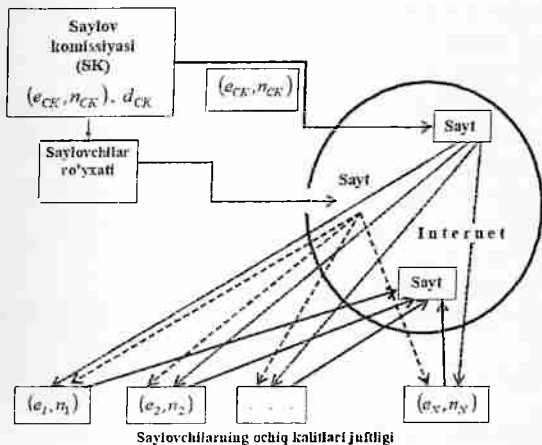
3. $M \rightarrow B: s, n^*, l, z$;

4. $B: d$ sonini hisoblaydi. (N, l) juftlik haqiqatan ham qiymati s so'm bo'lgan banknotligini tekshirib ko'radi. Maxsus qayd qilish registridan N nomerli banknot oldin ishlatilgan yoki ishlatilmaganligini

§10.2. Aloqaning telekommunikasiya kanallari bo'yicha ochiq kalitli kriptografiyaga asoslangan yashirin ovoz berish protokoli

Ushbu protokolni bardoshligi faktorlash va diskret logarifmlash masalalarining tez yechimini topishning imkonsizligiga asoslangan. Protokol quyidagi asosiy qismlardan tashkil topgan:

- protokolni inisializatsiyalash (dastlabki ma'lumotlarni taqsimlash);



10.1-rasm. Yashirin ovoz berish protokolini inisializatsiyalash.

- asosiy protokolni bajarish;
- asosiy protokolni korreksiyalash.

Ushbu qismlarni har birini bajarilishini ko'rib chiqamiz.

Protokolni inisializatsiyalash

Ushbu bosqichda quyidagi prosedurlar bajariladi (10.1-rasm):

1. SK saylovda qatnashish huquqiga ega bo'lgan saylovchilar ro'yxatini tuzadi;

10-BOB. YASHIRIN OVOZ BERISH PROTOKOLI VA UNING KRIPTOGRAFIK TAVSIFI

Ma'lumki, odatdagi yashirin ovoz berish jarayoniga nisbatan quyidagi talablar qo'yiladi:

1. Saylovlarda faqatgina Saylov komissiyasi (SK) ro'yxatiga oldindan kiritilgan, saylovda qatnashish huquqiga ega bo'lgan saylovchilarigina saylovda ishtirok etishi mumkin;

2. Saylovda qatnashish huquqiga ega bo'lgan har bir saylovchining ovoz berish natijasi saylov jarayonida ishtirok etuvchi barcha ishtirokchilar (shu jumladan, saylovda qatnashish huquqiga ega bo'lgan saylovchilar, SK a'zolari va saylovda qatnashmaydigan boshqa kishilar) dan sir tutilishi kerak;

3. Saylovda qatnashgan har bir ishtirokchining ovoz berish natijasi SK tomonidan to'g'ri hisobga olinishi va faqatgan bir marta hisobga olinishi lozim;

4. Saylovda qatnashish huquqiga ega bo'lmagan ishtirokchining SK ro'yxatida noto'g'ri qayd qilinganligi hamda ovoz berish natijasi SK tomonidan noto'g'ri hisobga olingan hollarda yashirin ovoz berish buzilmagan holatda ushbu xatolar to'g'rilanishi lozim;

5. Saylovda qatnashish huquqiga ega bo'lgan, ammo saylovda qatnashishni istamagan saylovchilar nomidan SK a'zolari qalbaki ovoz berishni tashkil qilish taqiqlanishi lozim.

Bu erda keltirilgan 3-5 talablarning bajarilishi saylovda qatnashish huquqiga ega bo'lgan saylovchilarning o'zlari ishtirokida amalga oshirilishi mumkin. Chunki ulardan boshqa hech kim ularning saylovda ishtirok etishini bilishi va ularning ovozlari to'g'ri hisobga olinishidan manfaatdor emas.

§10.1. Yashirin ovoz berish jarayoni

Avval yashirin ovoz berish kriptografik protokolini amalga oshirishda paydo bo'ladigan prinsipial qiyinchiliklarni ko'rib chiqamiz.

Telekommunikasiya kanallaridan foydalanib, yashirin ovoz berish protokolini amalga oshirishda sodir bo'ladigan eng katta muammo, yashirin ovoz berish natijalarini nafaqat tashkilotga, balki barcha foydalanuvchilarga shuningdek, ovoz berishda ishtirok etgan telekommunikasiya kanallaridan a'zolaridan sir tutilishini ta'minlash bilan bog'liq.

Yashirin ovoz berish natijalarini SKga uzatishning eng katta muammasi barcha foydalanuvchilardan tutib olinishidan iboratdir. Ma'lumotlarni SKga shifrlangan ko'rinishda uzatish eng ko'pincha mumkin. Ammo, bu yechim SKga aloqasiz ma'lumotlarni ta'minlaydi. Chunki, SK har bir qonuniy saylovchining ovoz berish natijalarini ta'minlash imkoniga ega bo'lishi, ammo, ammo bu natijalarni ta'minlashning eng katta muammasi orqali ovoz bergan saylovchilar bilan bog'liqdir. Ma'lumotlarni identifikatsiyalash imkoniyatiga ega bo'lmaydi. Ushbu muammoni echishda yagona imkoniyat mavjud. Bu imkoniyat aloqaning anonim kanalidan foydalanishdan iborat. Buning uchun ma'lumotlarni o'zgartirmasdan, SKga aniq uzatilgan ma'lumotlarni ma'lumotlarni jo'natuvchining manzilini aniqlashga imkon bermaydigan telekommunikasiya kanalini tashkirlash zarurdir. Quyidagilarni foydalanib, ushbu telekommunikasiya kanalini tashkil qilish mumkin:

- yozishma, jo'natmalarni anonimligini ta'minlaydigan protokollar.
- ma'lumotlarni anonim uzatish protokoli.

Bu keltirilgan vositalarni qo'llash quyidagi bir qator muammolar bilan sodir bo'ladi:

Birinchisi protokolda ovoz berish natijalarini hech kimga uzatish qilmaydigan, ishonchli «uchinchi shaxs» ishtirokini talab qiladi.

Ikkinchisi uzatish kanalini maxsus tashkil qilish barcha muammolar murakkab va ko'p vaqt talab qiladigan protokolni amalga oshirishni talab qiladi.

R.Sherwood tomonidan anonim kanal tashkil qilish bo'yida yangi yondoshuv taklif qilingan, ammo u hali qancha muammolar takomillashtirilmagan.

Bundan keyingi mulohazalarda anonim uzatish kanali mavjud bo'lgan faraz qilinadi hamda bu kanal yashirin ovoz berish prosedurasining komponentlaridan biri sifatida ishtirok etadi.

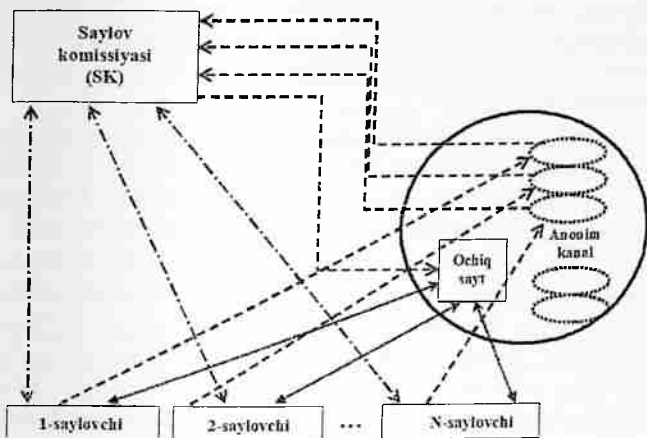
2. Saylovning har bir i -chi ishtirokchisi o'zining ochiq kaliti (e_i, n_i) va yopiq kaliti d_i ni generatsiya qiladi hamda ochiq kalitini Internet saytida e'lon qiladi;

3. SK ham o'zining ochiq kaliti (e_{CK}, n_{CK}) va yopiq kaliti d_{CK} ni generatsiya qiladi hamda ochiq kalitini Internet saytida e'lon qiladi.

Asosiy protokolni bajarilishi

Birinchi navbatda yashirin ovoz berish protokolini tashkil etuvchi qadamlarni sanab o'tamiz (10.2, 10.3-rasmlar):

1. SK barcha saylovchilarni ro'yxatini ochiq e'lon qiladi;
2. Saylovda ovoz berishni xohlagan saylovchilar o'zlarining ochiq kalitlari juftligini e'lon qiladi va o'zlari uchun identifikatsiya nomeri I ni generatsiya qiladi;
3. Saylovchi o'zining identifikatsiya nomeri (IN) ni niqoblaydi;
4. Saylovchi o'zining niqoblangan INni qo'shimcha kaliti yordamida shifrlab, SKga jo'natadi;
5. SK olingan xabarni dastlabki matnga o'giradi;
6. SK niqoblangan INni «ko'r-ko'rona» imzolaydi va saylovchiga jo'natadi;
7. Saylovchi «ko'r-ko'rona» imzolangan INdan niqobni olib tashlaydi;
8. Saylovchi o'zi uchun saylov byulletenini yaratadi va uni shifrlab, SKga aloqaning anonim kanali orqali jo'natadi;
9. SK qabul qilingan, shifrlangan xabarni e'lon qiladi;
10. Saylovchi shifrlangan xabarni dastlabki matnga o'girish uchun SKga anonim kanali orqali kalit jo'natadi;
11. SK saylovchi jo'natgan kalitdan foydalanib, qabul qilingan shifrlangan xabarni dastlabki matnga o'giradi va uni ovoz berish natijasi sifatida ochiq e'lon qiladi.



10.2-rasm. Yashirin ovoz berish protokolida axborot almashinuvi.

§10.3. Yashirin ovoz berish protokolini tashkil etuvchi qadamlar tavsifi

Protokolni qadamlarini batafsil ko'rib chiqamiz.

1-chi qadam. Saylovda ishtirok etuvchi saylovchilarning nomerlangan ro'yxatini SK o'zining yopiq kaliti yordamida imzolab, Internet saytida e'lon qiladi (ro'yxatni tuzishda odatdagi nomerlashdan farqli o'laroq, saylovchilar o'zlarini tez qidirib topishlari uchun saylovchilar ro'yxati boshqacha qoida bilan tuzilishi mumkin). Bunga qo'shimcha tarzda ovoz berish tartibi, protokolni har bir qadamini bajarilish vaqti va ovoz berish jarayonida saylovchilar almashinadigan axborotlarni tuzilmasi haqidagi axborotlar SK ning imzosi bilan tasdiqlangan shaklda e'lon qilinadi.

Ushbu qadamda yashirin ovoz berish protokolini amalga oshirishda ishtirok etuvchilarning protokolda ko'zda tutilmagan, zararkunandalik harakatlaridan protokolni himoyalash quyidagicha ta'minlanadi:

– SK a'zolari tomonidan himoyalash. SK saylovchilar ro'yxatini o'zining raqamli imzosi bilan imzolaydi, ya'ni ovoz berish huquqiga ega

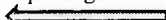
Hattoki, saylovchilar o'rtasida aloqaning anonim kanali mavjud bo'lsa-da, ammo bu yashirin ovoz berish protokolini bajarilishini to'liq hal qilmaydi. Gap shundaki, SK ovoz berish natijalarini qabul qilishda ushbu ma'lumotlar haqiqatan ham saylovda qatnashish huquqiga ega bo'lgan saylovchilar tomonidan jo'natilganligiga ishonch hosil qilishlari lozim. Ammo, ularni tekshirish saylovda ishtirok etganlarni o'zlarini identifikatsiyalash, ya'ni kim qanday ovoz berganliklarini aniqlash imkonini bermasligi lozim. Bu masala xuddi yechimi mavjud bo'lmagan ziddiyatli masalaga o'xshaydi. SHunday bo'lsa-da, bu masalani «ko'r-ko'rona» raqamli imzo protokolidan foydalanib, hal qilish mumkin. Bu haqda keyinroq fikr yuritiladi. Bundan tashqari 3-talabni bajarilishini ta'minlash ham zarur. Ushbu talab quyidagi ikkita talabga asoslangan:

- saylovda ishtirok etuvchi har bir qonuniy saylovchi bir martadan ortiq ovoz bermasligi lozim;

- saylovda ishtirok etuvchi har bir qonuniy saylovchining ovozi SK tomonidan hisobga olinishi lozim (ya'ni, berilgan ovoz yo'qotilishi mumkin emas).

4-talabga nisbatan shuni aytish mumkinki, ushbu talab nisbatan yumshoq bo'lib, bu holat qayta ovoz berishda sodir bo'ladi. Ushbu talab saylovchilarni ovoz berish natijalarini oshkor qilinishiga olib kelmasligi lozim.

5-talabni bajarilishida qiyinchiliklar paydo bo'lishi mumkin. SK saylovda qatnashish huquqiga ega bo'lgan, ammo saylovda ishtirok etmagan saylovchilar nomidan qalbaki ovoz berishni tashkil qitish natijasida o'ziga kerakli ovoz berish natijalariga erishishga urinishi mumkin. Agar protokolni bajarilish jarayonida saylovchi saylovda ishtirok etmasligini SKga rasmiy xabar qilmasa, SK uning ovozidan foydalanishga harakat qilishi mumkin. Buni SK osongina amalga oshirishi mumkin. Chunki, ovoz berishga SKning o'zi ruxsat beradi. Shu sababli protokolda saylovda ishtirok etmagan qonuniy saylovchilar ovozlardan SK foydalanish imkonini kamaytirishning ayrim proseduralari hisobga olingan. Ammo, bu muammoning to'liq yechimi saylovchilar tomonidan saylovda ishtirok etmasligi to'g'risida SKga xabar berishdan iborat.

Saylovchi tomonidan amalga oshiriladigan harakatlar (protokol qadamlari bo'yicha)	Axborot almashinuvidagi ma'lumotlarning harakatlanish yo'nalishi	Saylov komissiyasi (SK) tomonidan amalga oshiriladigan harakatlar (protokol qadamlari bo'yicha)
2-chi qadam Ochiq kalitni e'lon qilish va INni generatsiya qilish		1-chi qadam Ochiq kalitni va ovoz berish huquqiga ega bo'lgan saylovchilar ro'yxatini e'lon qilish
3-,4-chi qadamlar Niqoblangan INni hosil qilish	Niqoblangan IN shifrlangan ko'rinishda 	5-chi qadam Dastlabki matnga o'g'irish
	Imzolangan, niqoblangan INni 	6-chi qadam Niqoblangan INni imzolash
7-,8-chi qadamlar Niqobni echish, ovoz berish, kalitlarni yaratish	Shifrlangan byulleten  <i>Anonim kanal</i>	9-chi qadam Qabul qilingan shifrlangan byulletenlarni e'lon qilish
	10-chi qadam Byulletenlarni dastlabki matnga o'g'irish kaliti  <i>Anonim kanal</i>	11-chi qadam Byulletenlarni dastlabki matnga o'g'irish. Ovozlarni hisoblash. Natijalarni e'lon qilish

10.3-rasm. Yashirin ovoz berish protokolining asosiy bosqichlari.

SK a'zolari identifikatsiya nomeri *I* bilan byulletenni qabul qilgan vaqtda ushbu ishtirokchi ovoz berish huquqiga ega bo'lgan saylovchilardan biri ekanligiga ishonch hosil qilishlari lozim. Buning uchun identifikatsiya nomeri *I* unikalit bo'lishi talab etiladi. Ammo, na SK a'zolari, na boshqa biron ushbu saylovchiga qanday identifikatsiya nomeri *I* tegishli ekanligini

bo'lmagan ishtirokchilarni saylovchilar ro'yxatiga kiritishdan SK manfaatdor emas. Xuddi shuningdek, ovoz berish huquqiga ega bo'lgan ishtirokchilarni saylovchilar ro'yxatidan chiqarib tashlashga ham SK manfaatdor emas.

– *Saylovchilar tomonidan himoyalash.* Saylovchilar protokolda ko'zda tutilmagan harakatlarni amalga oshirmoqchi bo'lgan ishtirokchini SK ovoz berish huquqidan mahrum qilishini yaxshi biladilar. Shu sababli saylovchilar protokol qadamlarini to'g'ri amalga oshirishdan manfaatdor.

– *Ovoz berish huquqiga ega bo'lmagan begona shaxslardan himoyalash.* Ovoz berish huquqiga ega bo'lgan saylovchilar ro'yxatini SK imzolamaganida, buzg'unchilar ushbu ro'yxatni o'zgartirib qo'yishlari mumkin edi. Buning natijasida ovoz berish huquqiga ega bo'lgan saylovchilar ro'yxatda o'zlarini topmaganlaridan so'ng ular protest qilishlari yoki ularning ayrimlari ovoz berishni rad qilishlariga olib kelishi mumkin.

2-chi qadam. Saylovda ishtirok etishni istagan har bir saylovchi ovoz berish huquqiga ega bo'lgan saylovchilar ro'yxatidan o'zining familiyasi va nomerini topishi kerak (agar ushbu ro'yxatga o'zini kiritilmaganligini payqagan har bir saylovchi quyiroqda keltirilgan asosiy protokolni bajarilish korreksiyasi prosedurasiga ko'ra harakat qilishi lozim). Agar saylovchi o'zining familiyasi va nomerini ro'yxatdan topsa, u holda u umumiy uzunligi μ ta raqamdan tashkil topgan identifikasiya nomeri l ni tasodifiy generasiya qilishi kerak bo'ladi. Identifikasiya nomeri l ning uzunligi μ shunday tanlanadiki, ikki yoki undan ortiq saylovchilarning bir xil identifikasiya nomeri l ni tanlash ehtimoli e'tiborga olmaydigan darajada kichik bo'lishi lozim.

huquqiga ega bo'lgan saylovchilar ekanliklarini bilishi kerak. SHunday qilib, har bir i -chi saylovchi o'zining nomeri n ni va niqoblangan identifikatsiya nomeri I (ya'ni, I_m) ni o'zining yopiq kaliti d_i dan foydalanib, shifrlaydi.

Har bir i -chi saylovchi ochiq aloqa kanali orqali quyidagi xabarni SKga jo'natadi:

$$M_i = (n, E_{d_i}(n, I_m)),$$

bu erda n saylovchining hamma uchun ochiq bo'lgan saytdagi saylovchilar ro'yxatidagi nomeri, $E_{d_i}(n, I_m)$ asimmetrik shifrlash tizimidan foydalanib, saylovchi o'zining yopiq kaliti d_i dan foydalanib, (n, I_m) xabarni shifrlaganini anglatadi. Ushbu xabarda faqatgina identifikatsiya nomeri yashirilgan, saylovchining nomeri n esa saylovchilar ro'yxati orqali SKga ma'lum.

Agar buzg'unchi saylovchi nomidan xabarni imzolatish uchun jo'natishni xohlasa, u buni uddalay olmaydi. Chunki, u saylovchining yopiq kalitini bilmaydi.

5-chi qadam. SK barcha qabul qilingan M_i xabarlarni ochiq saytda e'lon qiladi. Undan so'ng SK barcha kriptogrammalarni dastlabki matnga o'giradi. Buning uchun ochiq saytda joylashtirilgan saylovchining ochiq kaliti juftligi (e, n_i) hamda saylovchining nomeri n dan foydalanadi. Agar M_i xabarni tiklashdan hosil bo'lgan n sonining qiymati M_i xabarni ochiq qisidagi n sonining qiymati bilan mos kelsa, u holda SK ushbu xabar haqiqatan ham i -chi saylovchidan kelganligiga ishonch hosil qiladi.

M_i xabarlarni ochiq saytda e'lon qilish ovoz berish huquqiga ega bo'lgan saylovchilardan qaysilari ovoz bermasligini bilish uchun kerak. SK ovoz berishda ishtirok etmagan saylovchilar hisobidan ovozlarni soxtalashtirish imkoniga ega bo'lmasligi lozim. M_i xabarlar ochiq saytda e'lon qilinmasa, SK saylov jarayoni va ovoz berish natijalarini soxtalashtirish imkoniga ega bo'ladi. M_i xabarlarni hosil qilishda saylovchilarning yopiq kalitlari d_i lardan foydalaniladi, shu sababli bu xabarlarni soxtalashtirish mumkin emas. Demak, M_i xabarlarni ochiq saytda e'lon qilinishi ovoz beruvchilarni aniqlash imkoni ta'minlaydi va

bilmasliklari kerak. Aks holda ushbu saylovchining ovoz berish natijasi oshkor bo'lib qoladi.

SK ushbu ishtirokchi ovoz berish huquqiga ega bo'lgan saylovchilardan biri ekanligini bilish uchun saylovchining identifikatsiya nomeri I qo'llanilgan. Ushbu protokolda identifikatsiya nomeri I ni saylovchining o'zi hosil qiladi va imzolash uchun uni SK ga jo'natadi. SK tomonidan imzolangan identifikatsiya nomeri saylov kompaniyasida ovoz berish huquqining etarlicha belgisidir. Bu erda muammo shundaki, identifikatsiya nomerining egasi ovoz berish huquqiga ega bo'lgan saylovchi ekanligiga SK ishonsada, ammo qanday nomerli identifikatsiya nomerini imzolayotganligini SK bilmasligi kerak. Ushbu muammo «ko'r-ko'rona» elektron raqamli imzo vositasida hal qilinadi.

3-chi qadam. «Ko'r-ko'rona» raqamli imzoni yaratishning turli usullari mavjud. Ushbu usullardan birini ko'rib chiqamiz. Identifikatsiya nomeri I niqoblovchi ko'paytuvchiga, ya'ni r soniga ko'paytiriladi. Bu ko'paytuvchini keyinroq qisqartirishga to'g'ri keladi, shu bois uning SKning ochiq kaliti darajasi $r^{e_{CK}}$ oldindan hisoblanadi. Saylovchi identifikatsiya nomeri I ni SK ga «ko'r-ko'rona» imzolatish uchun oldindan niqoblab qo'yadi. Buning uchun u quyidagi almashtirishni bajaradi:

$$I_r = r^{e_{CK}} \cdot I \bmod n_{CK}. \quad (10.1)$$

Bu erda (e_{CK}, n_{CK}) - SKning barchaga ma'lum bo'lgan ochiq kalit juftligi, $r - 1 < r < n_{CK}$ shart bo'yicha tasodifiy tanlanadigan, n_{CK} bilan o'zaro tub bo'lgan son bo'lib, niqob vazifasini bajaradi.

Saylovchining niqoblangan identifikatsiya nomeri I_m dan identifikatsiya nomeri I ni aniqlashi uchun r ning barcha qiymatlarini saralab ko'rishi talab etiladi. Bu masala amalda imkonsiz masala, chunki n_{CK} juda katta son bo'lganligi sababli identifikatsiya nomeri I ni haqiqiy qiymatini aniqlash mushkul masala.

Tashqaridagi kuzatuvchi ham SK singari niqoblovchi ko'paytuvchi r ning qiymatini bilmaydi, shu sababli u ham identifikatsiya nomeri I ni haqiqiy qiymatini bilish imkoniga ega emas.

4-chi qadam. SK har bir haqiqiy saylovchining bittadan identifikatsiya nomeri I ni imzolashi uchun ushbu saylovchilar ovoz berish

Agar ushbu tenglik bajarilmasa, saylovchi o'zining e'tirozini SKga bildiradi va undan to'g'ri imzolashni talab qiladi (qo'yiroqda asosiy protokoldagi xatolikni to'g'rilash keltiriladi).

Shunday qilib, barcha ovoz berish huquqiga ega bo'lgan saylovchilar 7-chi qadamdan so'ng SK tomonidan imzolangan haqiqiy identifikatsiya nomerlari I ga ega bo'ladi. Bu esa ularni protokolni keyingi qadamlarini bajarishga haqli ekanliklarini tasdiqlaydi. Boshqa tomondan olganda, SK saylovchilarning identifikatsiya nomerlarini niqoblangan holda imzolagani uchun ushbu nomerlarni bilmaydi.

8-chi qadam. Saylovchilar saylovdagi o'z ovozlari natijalarini V xabar ko'rinishida shakllantiradilar. Undan so'ng ovoz berish natijalarini shifrlash/dastlabki matnga o'girish uchun har bir i -chi saylovchi o'zining ochiq kaliti juftligi (e_i, n_i) va yopiq kaliti d_i ni generatsiya qiladilar. Saylovchilarning har biri quyidagi M_2 xabarni shakllantiradilar:

$$M_2 = (P, E_{d_i}, (I, I_s, V)).$$

Bu erda P - M_2 xabarni ochiq saytdan oson qidirib topish uchun foydalaniladigan ixtiyoriy son (ushbu son bir necha saylovchilar uchun bir xil bo'lishi ham mumkin). Saylovchi M_2 xabarni anonim kanal orqali SKga jo'natadi. (I, I_s, V) xabarlarni shifrlangan holda jo'natilishini quyidagicha izohlash mumkin. Agar ushbu xabarlar ochiq holda, masalan, $M_2' = (P, I, I_s, V)$ ko'rinishda jo'natilganida SK o'z imzosining haqiqiylikiga ishonch hosil qilishi va ovoz berish natijasi V ni haqiqiy deb hisoblagan bo'lar edi. Ammo, bunda M_2' xabarni butunligini buzilishiga buzg'unchi tomonidan xavf mavjud edi. Masalan, buzg'unchi M_2'' xabarni $M_2'' = (P, I, I_s, V')$ xabar bilan almashtirib qo'yishi mumkin edi. Bu erda $V' \neq V$ boshqa ovoz berish natijasiga mos keladi. Ovozni bunday almashtirilganini SK payqamasligi mumkin edi.

Shunday qilib, SK M_2 xabarni kim jo'natganini bilmaydi, chunki saylovchilar ushbu xabarni jo'natishda anonim kanaldan foydalanadilar. Agar ushbu xabar ovoz berish huquqiga ega bo'lmagan shaxsdan jo'natilganida ham SK xabarni dastlabki matnga o'girgandan keyingina bu haqida biladi.

halol bo'lmagan SKni ovoz berish natijalarini soxtalashtirish imkonini yo'qqa chiqaradi. Bu esa juda muhim, chunki saylovchilarning ovoz berishni rad qilgan kattagina qismi identifikasiya nomerlarini generatsiya qilmaydi va SKga ularni jo'natmaydi.

6-chi qadam. Agar saylovchi haqiqatan ham ovoz berish huquqiga ega bo'lsa, u holda SK uni niqoblangan identifikasiya nomeri I_m ni imzolaydi. Masalan, RSA raqamli imzodan foydalanib, quyidagicha imzolaydi:

$$I_{sm} = I_m^{d_{CK}} \bmod n_{CK}.$$

Undan so'ng SK I_{sm} ni ochiq kanali bo'yicha n -chi saylovchiga jo'natadi hamda barcha saylovchilar ko'rishi mumkin bo'lgan saytda saylovchining nomeri n bilan birgalikda joylashtiradi. Agar SK buni xohlamagan taqdirda ham u xabarni imzolashi va uni saylovchiga albatta jo'natishi lozim bo'ladi. Chunki, SK tomonidan qilingan ixtiyoriy aldev yoki soxtakorlik fosh bo'ladi.

Boshqa tomondan imzolangan xabarni saylovchi rad qila olmaydi. Niqoblangan identifikasiya nomeri I_m barcha saylovchi uchun ochiq bo'lgan saytda tursa-da, niqoblovchi ko'paytuvchisiz identifikasiya nomerini haqiqiy qiymatini aniqlashning imkoni yo'q.

7-chi qadam. Saylovchilar SK tomonidan niqoblangan identifikasiya nomeri I_m ga mos keluvchi I_{sm} imzodan haqiqiy identifikasiya nomeri I ga mos keluvchi I_s imzoni quyidagicha shakllantira oladilar:

$$I_s = (I_{sm} / m) \bmod n_{CK}.$$

Buni to'g'riligini quyidagicha tekshirib ko'rish mumkin:

$$\begin{aligned} I_{sm} / m &= I_m^{d_{CK}} \bmod n_{CK} \cdot m^{-1} \bmod n_{CK} = (m^{e_{CK}})^{d_{CK}} \cdot I^{d_{CK}} \cdot m^{-1} \bmod n_{CK} = \\ &= m \cdot I^{d_{CK}} \cdot m^{-1} \bmod n_{CK} = I^{d_{CK}} \bmod n_{CK} = I_s. \end{aligned} \quad (*)$$

(*) amallarni bajargandan so'ng, saylovchi SKning ochiq kalitidan foydalanib, uning imzosini to'g'riligini tekshirib ko'radi:

$$(I^{d_{CK}})^{e_{CK}} \bmod n_{CK} = I.$$

§10.4. Yashirin ovoz berish protokoliga qo'shimcha sharhlar

8-chi va 10-chi qadamlarda anonim kanallardan albatta foydalanish zarur. Aks holda SK identifikatsiya nomeri I kimga tegishli ekanligini bilishi va ovoz berish natijalarini sirligi buzilishi mumkin.

Agar saylovchi 4-chi qadamni bajarsada, keyinchalik ovoz berishni xohlamasa, u holda ushbu saylovchi bu haqda SK ni xabardor qilishi lozim. Ushbu holatda saylovchi quyidagi xabarni shakllantiradi:

$$M_a = (n, E_d, (n, R, I, I_s)),$$

bu erda n - saylovchining nomeri; R - oldindan qiymati belgilanadigan, saylovchini ovoz berishdan bosh tortishini anglatuvchi alomat; I - identifikatsiya nomeri, xabarda bo'lmashligi ham mumkin; I_s - imzolangan identifikatsiya nomeri, xabarda bo'lmashligi ham mumkin; $E_d(n, R)$ - (n, R) xabarni saylovchining yopiq kaliti bilan shiflangan kriptogrammasi. Saylovchi ushbu xabarni SKga jo'natadi. Bundan tashqari oldindan soni aniqlangan saylovchilarni tanlaydi va ularning har biriga o'zining xohishiga ko'ra M_a xabarni jo'natadi. Ovoz berish natijalarini e'lon qilishda SK ovoz berishni rad qilgan saylovchilar o'hrisidagi qo'shimcha axborotni ham saylovchilarga taqdim qiladi. Agar saylovchi SK tomonidan imzolangan identifikatsiya nomeri I_s ni olsa, u holda bu identifikatsiya nomeri foydalanilmasligi uchun uni albatta ochishi kerak.

Nohalol SK saylov kompaniyasi boshidan ishtirok etmagan saylovchilar nomidan ovoz berish natijalarini soxtalashtirishi mumkin emas. Chunki, ovoz beruvchi saylovchi protokolni 4-chi qadamida M_1 xabarni SKga jo'natib, o'zining saylovda ovoz berishga xohishi borligini tasdiqlaydi. Bunday xabarni SK yaratish imkoniga ega emas, chunki buning uchun saylovchining yopiq kalitini bilishi kerak bo'ladi. Ovoz berishni rad qilgan saylovchilarning kattagina qismi saylov kompaniyasi boshidan ovoz berishni rad qilishgan deb hisoblash o'rinli. Biroq, saylovchilarning kichik qismi protokolni 4-chi qadamini bajarib, keyinchalik protokolni ixtiyoriy qadamida (11-chi qadamdan boshqa) saylovni davom ettirish, ovoz berishda ishtirok etishni rad qiladilar. 4-chi

Saylovchi faqatgina imzolangan bitta identifikatsiya nomeriga ega bo'lganligi sababli bor yo'g'i bir marta ovoz berishi mumkin.

Faqatgina imzolangan identifikatsiya nomeriga ega bo'lganlarga bunday xabarlarini shakllantirishlari mumkin. Boshqa barcha xabarlar SK tomonidan protokolning keyingi qadamlarida haqiqiy emas deb hisoblanadi.

9-qadam. SK M_2 xabarni (shifrlangan holda) ochiq saytda e'lon qiladi.

10-qadam. Saylovchilar anonim kanal orqali M_3 xabarni SKga quyidagi ko'rinishda jo'natadilar:

$$M_3 = (P, e, n_i).$$

SK ushbu xabarni qabul qilib, M_2 xabarni dastlabki matnga o'girishi mumkin. Natijada SK unga noma'lum, ammo ovoz berish huquqiga ega bo'lgan (chunki uning identifikatsiya nomeri SK tomonidan imzolangan) saylovchining ovoz berish natijasini hisobga oladi. Agar ushbu ovoz nohalol SKni qanoatlantirmasa, u holda SK ushbu ovozni inkor qilishga harakat qilishi mumkin (qo'yiroqda asosiy protokoldagi xatolikni to'g'rilash keltiriladi, 4-chi situatsiya).

Ko'rinish turibdiki, identifikatsiya nomeri SK tomonidan imzolangan shaxs M_3 ga o'xshash xabarni SKga jo'natishi mumkin. Ammo, uning ovoz berish natijasi SK tomonidan e'tiborga olinmaydi.

11-qadam. SK i -chi saylovchining ochiq kaliti juftligi (e, n_i) dan foydalanib, uning M_2 xabarini dastlabki matnga o'giradi. Natijada SK I, I, V ga ega bo'lib, ovoz berish natijasini haqiqiylikiga ishonch hosil qiladi, ochiq ko'rinishda hosil qilingan ovoz berish natijasi V ni hisobga olib, har bir saylovchi o'zining ovoz berish natijasi to'g'ri hisobga olinganligini tekshirishi uchun ochiq saytda identifikatsiya nomeri bilan birgalikda e'lon qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Akbarov D.Y. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi. –Т., O'zbekiston markasi. 2009. – 432 b.

2. Агибалов Г.П. Избранные теоремы начального курса криптографии: Учебное пособие. – Томск: Изд-во НТЛ, 2005. – 116 с.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.

4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М.: Горячая линия–Телеком, 2004. – 212 с.

5. Введение в криптографию /Под общей ред. В.В. Ященко. – М.: МЦНМО, 1998. – 272 с.

6. Виноградов И. М. Основы теории чисел. – М.: Наука, 1972. – 402 с.

7. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. Учебное пособие для вузов. –М.: Горячая линия. –Телеком, 2007. – 320 с.

8. Зубов А.Ю. Математика кодов аутентификации /А.Ю.Зубов. – М. : Гелиос АРВ, 2007.

9. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Изд-во «Лань», 2001. – 224с.

10. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ-Петербург, 2005. – 288 с.

11. Ниссенбаум О.В. Криптографические протоколы. Учебное пособие. – Тюмень, 2007. – 140 с.

12. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. – М.: Горячая линия–Телеком, 2005. – 229 с.

13. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие. М.: Изд. Центр «Академия», 2009. – 272 с.

qadamdan so'ng saylovchi SKga anonim kanal orqali murojaat qiladi, buning natijasida SKga kim xabar jo'natayotganini aniqlash imkoni bo'lmaydi. Bu esa ovoz berish huquqiga ega bo'lmagan yoki g'irromlik qiluvchi shaxslar ham SKga xabar jo'natishga harakat qiladi degan fikrga olib kelishi mumkin. Ammo, bunday shaxslarning ovozi hisobga olinishi uchun SK tomonidan imzolangan identifikasiya nomeri *I*, dan foydalanish lozim bo'ladi.

4-chi qadamdan so'ng saylovda ishtirok etishni xohlamagan saylovchilar nomidan SK qalbaki identifikasiya nomerlarini yaratishi mumkin. Ushbu holatda saylovni davom ettirishni xohlamagan saylovchilar o'zlarini niqobni echishdan hosil bo'lgan identifikasiya nomerlari imzolarini ovoz berishda ishtirok etmaganliklari isboti sifatida taqdim qilsalar, SK tomonidan qilingan aldovni fosh qilish mumkin. Agar identifikasiya nomerlari imzolari taqdim qilinmasa, SK tomonidan qilingan aldovni fosh qilish imkoni yo'qqa chiqadi.

29. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. Учебное пособие для вузов. –М.: Горячая линия. –Телеком, 2007. – 320 с.

30. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. – 400 с.: ил.

31. Ниссенбаум О.В. Криптографические протоколы. Учебное пособие. – Тюмень, 2007. – 140 с.

32. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. – М.: Горячая линия–Телеком, 2005. – 229 с.

33. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. –Т., ФТМТМ, 2008. – 208 б.

34. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. –Т., Алоқачи, 2008. –282 б.

35. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие. –М.: Изд. Центр «Академия», 2009. – 272 с.

36. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003 – 816 с.

14. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003 – 816 с.,

15. Index of the security protocols repository (SPORE) // Laboratoire Spécification et Vérification. <http://www.lsv.ens-cachan.fr/spore/table.html>.

16. Clark J., Jacob J. A Survey of Authentication Protocol Literature: Version 1.0. 17 Nov. 1997.

17. <http://www.cs.york.ac.uk/jac/papers/drareview.ps.gz>, 1997.

18. Menezes A. J., van Oorschot P.C., Vanstone S.A. Handbook of applied cryptography. BocaRaton, New York, London, Tokyo: CRC Press, 1997. - 780 p.

19. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1996. – 661 p.

20. Oehl F. Automatic Approximation for the Verification of Cryptographic Protocols / F. Oehl, G. Cece, O. Kouchnarenko // Proc. Int. Conf. on Formal Aspects of Security (FASec). — London, 2003. — Lecture Notes in Computer Science. - V. 2629. - P. 33-48.

21. Cremers C. J. F., Lafourcade P. Comparing State Spaces in Automatic Security Protocol Verification. ETH Technical Report. 2007. No. 558. – 26 p.

22. Diffie W., Hellman M.E. New directions in cryptography //IEEE Transactions on Information Theory. – 1976. – V. 22. P.644-654.

23. Goldwasser S., Bellare M. Lecture notes on cryptography. – Cambridge, Massachusetts, 2001. – 283 p.

24. Stinson D.R.: Cryptography, theory and practice. -London etc., CRC Press, 1995.

25. <http://geo.com.ru/db/msg.html?mid=1161287&uri=all.html>.

26. Akbarov D.Y. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi. –T., O'zbekiston markasi. 2009. – 432 b.

27. Aripov M.M., Abdurahimov B.F., Matyakubov A.S. Kriptografik usullar. –T., Universitet. 2020. –176 b.

28. Jo'rayev G.U. Kriptografik protokollar. –T., Fan va texnologiyalar. 2016. –142 b.

JO'RAYEV G'AYRAT UMAROVICH

KRIPTOGRAFIK PROTOKOLLAR

O'quv qo'llanma

Muharrir Z.N.Buranov

Bosishga ruxsat etildi 12.12.2022y. Bichimi 60X84 $\frac{1}{16}$.
Bosma tabog'i 10,0. Shartli bosma tabog'i 10,0. Adadi 30 nusxa.
Buyurtma № 78. Bahosi kelishilgan narxda.
"Universitet" nashriyoti. Toshkent, Talabalar shaharchasi,
O'zMU ma'muriy binosi.
O'zbekiston Milliy universiteti bosmaxonaşida bosildi.
Toshkent, Talabalar shaharchasi, O'zMU.