

KRIPTOGRAFIK PROTOKOLLAR VA ULARNING AXBOROT XAVFSIZLIGINI TA'MINLASHDAGI O'RNI

Umarov Nurali Olimjonovich

Annotatsiya: *Ushbu maqolada zamonaviy raqamli makonda axborot xavfsizligining poydevori hisoblangan kriptografik protokollarning nazariy-uslubiy asoslari va funksional arxitekturasini chuqur tahlil qilingan. Tadqiqot davomida shifrlash, autentifikatsiya, butunlikni saqlash va inkor etilmaslik kabi xavfsizlik mexanizmlarining ishlash tamoyillari hamda ularning TLS, IPsec, SSH, PGP protokollari misolidagi amaliy tatbiqi yoritilgan. Shuningdek, simmetrik va asimmetrik tizimlardagi matematik hamda implementatsion zaifliklar tasniflanib, an'anaviy tahlil usullarining cheklanganligi va bu borada sun'iy intellekt (Machine Learning) usullarini qo'llashning ilmiy zarurati asoslab berilgan.*

Kalit so'zlar: kriptografik protokol, axborot xavfsizligi, maxfiylik, yaxlitlik, autentifikatsiya, simmetrik va asimmetrik shifrlash, raqamli imzo, zaifliklar tahlili, sun'iy intellekt, Machine Learning, Deep Learning.

Bugungi kunda axborot-kommunikatsiya tizimlari hayotning barcha sohalarida chuqur integratsiyalashgan bo'lib, ular orasida moliyaviy operatsiyalar, davlat xizmatlari, sanoat boshqaruv tizimlari, shaxsiy ma'lumotlar almashinuvi kabi jarayonlar alohida o'rin egallaydi. Mazkur tizimlarda uzatilayotgan ma'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasi kriptografik protokollar orqali ta'minlanadi. Biroq amaliyot shuni ko'rsatadiki, kriptografik algoritmlar matematik jihatdan barqaror bo'lgan taqdirda ham, ularning protokol darajasidagi noto'g'ri loyihalaniishi, implementatsiya xatolari yoki noto'g'ri sozlanishi tufayli zaifliklar yuzaga kelishi mumkin.

Kriptografik protokollarning umumiy qoidasi shundan iboratki, protokolda belgilanganidan ortiqcha harakatlarni qilish yoki axborotlarni bilish mumkin emas. Hozirgi vaqtda axborot xavfsizligiga doir turli masalalarni ijobiy hal qilishda kriptografik protokollar muvaffaqiyatli qo'llanib kelmoqda. An'anaviy yondashuvlarda kriptografik protokollar zaifliklari asosan formal verifikatsiya usullari, kuzatilgan hujum ssenariylari tahlili yoki qo'lda tekshirish orqali aniqlab kelingan. Biroq tarmoqlar va protokollar murakkablashib borayotgan hozirgi sharoitda ushbu yondashuvlar ko'p vaqt talab etishi va masalaning dinamik tabiatini yetarlicha qamrab ololmasligi mumkin. Shu nuqtai nazardan Machine Learning va Deep Learning usullariga asoslangan yondashuvlar kriptografik protokollardagi zaifliklarni aniqlash va proaktiv himoya choralarini ko'rishda istiqbolli yo'nalishlardan biri hisoblanadi.

Kriptografik protokollar – bu ikki yoki undan ortiq sub'ektlar o'rtasida ma'lumot almashinuvi jarayonida xavfsizlik xususiyatlarini ta'minlash uchun oldindan

belgilangan qoida va algoritmlar ketma-ketligidir. Masalan, SSL/TLS, IPsec, SSH kabi protokollar internet muhitida keng qo'llaniladi. Bunday protokollarning asosiy maqsadi ma'lumotlarni shifrlash, ishtirokchilarni autentifikatsiya qilish, xabar yaxlitligini ta'minlash va hujumlardan himoyalashdir. Shu bilan birga, protokollardagi kichik dizayn xatolari yoki implementatsiya kamchiliklari turli zaifliklarga sabab bo'lishi mumkin. Ular orasida man-in-the-middle (MITM) hujumlari, qayta uzatish (replay) hujumlari, yon kanalli (side-channel) hujumlar, noto'g'ri kalit boshqaruvi, sertifikatlarni tekshirishdagi xatoliklar va boshqa ko'plab muammolarni keltirish mumkin. Ko'plab tarixiy voqealar shuni ko'rsatadiki, zaifliklar ko'pincha protokolning matematik zamiridan emas, balki uning amaliy qo'llanishidagi xatolar tufayli yuzaga keladi.

Kriptografik protokollarni turli mezonlarga ko'ra tasniflash mumkin. Masalan:

- Maqsadiga ko'ra: kalit almashinuv protokollari, autentifikatsiya protokollari, sessiya boshqaruv protokollari va h.k.
- Qo'llanilish sohasiga ko'ra: tarmoq darajasidagi protokollar (IPsec), transport darajasidagi (TLS), ilova darajasidagi (PGP) va boshqalar.
- Kalitlar turiga ko'ra: simmetrik kalitga asoslangan protokollar, ochiq kalitli (asimmetrik) protokollar yoki gibril protokollar.

Har bir toifa o'ziga xos dizayn tamoyillariga ega bo'lib, ularda uchrashi mumkin bo'lgan zaifliklar ham maqsad va arxitekturaga qarab farqlanadi. Shu sababli ML va DL yondashuvlarini qo'llashdan oldin protokolning turini, qatlamini va asosiy vazifalarini aniq belgilab olish muhimdir.

Kriptografik protokollarning funksional vazifalaridan birinchisi maxfiylik vazifasi hisoblanadi. Protokollar ma'lumotlarni shifrlash orqali uni faqat ruxsat etilgan foydalanuvchilar o'qiy olishini ta'minlaydi.

Ta'rif: Maxfiylik – bu ma'lumotni faqat ruxsat etilgan tomonlar o'qiy olishi, boshqa hech kim mazmunini tushuna olmasligidir. Ya'ni, kanalni tinglayotgan hujumchi paketlarni ko'rishi mumkin, lekin ularni tushunolmasligi kerak. Shuning uchun protokollar ma'lumotni shifrlangan ko'rinishda uzatadi. Kriptografik protokollarda maxfiylik asosan shifrlash algoritmlari orqali ta'minlanadi. Quyida shifrlash algoritmlarini qo'llanilishi, vazifalari haqida to'xtalamiz.

Simmetrik shifrlash (bir xil kalit). Simmetrik shifrlashda bitta kalit ham shifrlash, ham deshifrlash uchun ishlatiladi. Bu algoritmni ishlash tezligi yuqori bo'lib o'z navbatida katta hajmdagi ma'lumot uchun qulay hisoblanadi. Bunday shifrlash algoritmlariga misol qilib AES, DES (eskirgan), 3DES larni keltirish mumkin. TLS, IPsec, SSH kabi protokollarda, seans kaliti (session key) o'rnatilgandan so'ng, uzatilayotgan asosiy ma'lumotlar oqimini shifrlash uchun aynan simmetrik algoritmlardan foydalaniladi, chunki ular asimmetrik algoritmlardan minglab marta tezroq ishlaydi.

Asimmetrik Shifrlash (Asymmetric Encryption). Bu algoritmda bir vaqtning o'zida ikkita alohida kalit (ochiq va yopiq kalit) ishlatiladi. Ular odatda kichik hajmdagi

ma'lumotni (odatda, simmetrik kalitni) shifrlash uchun ishlatiladi. Maxfiylikni ta'minlashda bu algoritmlar to'g'ridan-to'g'ri asosiy ma'lumotni shifrlash uchun kamdan-kam qo'llaniladi. Ularning asosiy vazifasi – simmetrik shifrlash uchun ishlatiladigan seans kalitini (Session Key) xavfsiz va maxfiy ravishda almashishdir. Bunday shifrlash algoritmlariga misol qilib RSA, ECC (Elliptik egri chiziqlar kriptografiyasi)larni keltirish mumkin.

Maxfiylik vazifasi protokollarning turli qatlamlarida har xil darajada qo'llaniladi. Quyidagi jadvalda maxfiylik vazifasini protokollarning turli qatlamlarida qo'llanilishi keltirilgan:

Protokol	Qo'llanilish turi	Maxfiylikni ta'minlovchi Algoritm
TLS/SSL (Transport Qatlami)	Veb-trafik (HTTPS), elektron pochta.	AES-GCM yoki ChaCha20/Poly1305
IPsec (Tarmoq Qatlami)	VPN ulanishlari, butun tarmoq trafigini shifrlash.	AES (ESP rejimida)
SSH (Ilova Qatlami)	Masofaviy buyruqlar, fayl uzatish.	AES-CTR
PGP/GPG (Ilova Qatlami)	Xabarlar, fayllar.	Gibrid (RSA bilan AES kalitini shifrlash)

Kriptografik protokolning maxfiyligi buzilgan taqdirda, hujumchi ma'lumotlarni o'qish imkoniyatiga ega bo'ladi. Asosiy tahdidlar quyidagilardir:

- Eavesdropping (Tinglash): Hujumchi uzatish kanalidan o'tayotgan shifrlangan ma'lumotlarni yashirincha nusxalab olishi. Maxfiylik ushbu ma'lumotni tushunarsiz holatda saqlaydi.
- Known-Plaintext Attack (Ma'lum Ochiq Matn Hujumi): Hujumchi bir nechta ochiq matn va uning mos shifr matnini bilsa, shifrlash mexanizmidagi zaiflikni topishga urinishi.
- Brute-Force Attack: Shifrlangan ma'lumotni ochish uchun mumkin bo'lgan barcha kalitlarni sinab ko'rish. AES-256 kabi algoritmlar hozirgi kompyuterlar uchun bunga chidamli.
- Kalitni o'g'irlash/Komprometatsiya: Agar shifrlash uchun ishlatiladigan kalit (ayniqsa, yopiq kalit) hujumchiga ma'lum bo'lsa, maxfiylik butunlay yo'qoladi.

Maxfiylik faqatgina shifrlash algoritmining matematik kuchi bilan cheklanmaydi. Protokol darajasida quyidagilar ham muhim:

- IV (Initialization Vector) / Nonce: Blokli shifrlash rejimlarida (masalan, AES-CBC yoki AES-GCM) IV yoki Nonce kabi tasodifiy (yoki bir marta ishlatiladigan) qiymatlardan foydalanish shart. Agar bu qiymatlar noto'g'ri takrorlansa, bir xil kalit

bilan shifrlangan turli matnlar orasidagi bog'liqlik yuzaga keladi va bu maxfiylikni buzadi (masalan, BEAST hujumi).

- Perfect Forward Secrecy (PFS): Ushbu xususiyat (ko'pincha Diffie-Hellman orqali ta'minlanadi) agar asosiy uzoq muddatli yopiq kalit (masalan, serverning RSA kaliti) buzilsa ham, o'tmishdagi seans kalitlarining maxfiyligini saqlab qolishni kafolatlaydi.

Xulosa qilib aytganda maxfiylikni to'liq ta'minlash — bu nafaqat mustahkam shifrlash algoritmini tanlash, balki protokolning barcha talablariga (kalit almashinuvi, IV/Nonce boshqaruvi) qat'iy rioya qilishni ham talab qiladigan murakkab jarayondir.

Ko'pchilik zamonaviy protokollar ikkalasini ham aralashtirib ishlatadi. Buning uchun avval asimmetrik kriptografiya orqali: sessiya uchun tasodifiy simmetrik kalit almashiladi. So'ngra butun real ma'lumot almashinuvi shu simmetrik kalit bilan shifrlanadi. Gibrid kriptografiya — bu simmetrik va asimmetrik shifrlash tizimlarining eng yaxshi tomonlarini birlashtirgan yondashuv bo'lib, ularning kamchiliklarini bartaraf etadi. Bu usul zamonaviy xavfsiz protokollarning deyarli barchasida qo'llaniladi.

Gibrid kriptografiya zamonaviy axborot xavfsizligining oltin standarti hisoblanadi. U xavfsizlikni asimmetrik kriptografiya orqali ta'minlaydi, tezlikni simmetrik kriptografiya orqali ta'minlaydi, masshtablanuvchanlikni sessiya kalitlari orqali ta'minlaydi, *Forward secrecy* ni ephemeral kalitlar orqali ta'minlaydi

Aynan shu kombinatsiya TLS, SSH, IPsec, WireGuard va boshqa zamonaviy protokollarning muvaffaqiyatining asosiy sababidir.

Misol: TLS (https)

- Browser sayt sertifikatini (ochiq kalitni) olib, simmetrik sessiya kalitini RSA/Diffie-Hellman orqali “yashirincha” uzatadi.

- Keyingi barcha ma'lumotlar AES bilan shifrlanadi.

Maxfiylikni ta'minlashda bundan tashqari qo'shimcha usullar ham mavjud. Quyida ularni ishlash rejimlariga to'xtalamiz:

Blok shifrlash rejimlari. Simmetrik blok shifrlagichlar (masalan AES) rejimlar bilan ishlaydi:

- ECB (Electronic Code Book) – xavfsiz emas, bir xil blok → bir xil shifr-blok.
- CBC (Cipher Block Chaining) – har bir blok oldingi blokka bog'liq, biroz xavfsizroq.
- CTR, GCM – tezkor va xavfsiz rejimlar, TLS, IPsec kabi protokollarda ko'p uchraydi.

Maxfiylik uchun muhim: rejim noto'g'ri tanlansa, shifr ma'lum darajada “namuna” (pattern) saqlab qolishi va hujumchi analiz qilishi mumkin.

IV (Initialization Vector) va nonce

- IV – boshlang'ich vektor, ko'pincha tasodifiy bo'lishi kerak.

• U bir xil bo'lmaganligi sababli, bir xil ma'lumot ham har safar har xil shifrlangan ko'rinish beradi.

• Maxfiylikni kuchaytiradi, chunki hujumchi “bir xil xabar – bir xil shifr” naqshini ko'ra olmaydi.

Sessiya kalitlari

• Protokollar odatda har bir sessiya uchun alohida kalit ishlab chiqaradi.

• Bunga forward secrecy (oldingi sessiyalar sirini saqlab qolish) ham bog'liq: Agar keyinchalik bitta kalit qo'lga tushsa ham, hamma eski sessiyalar ochilmasligi kerak.

Amaliyotda maxfiylikning ta'minlashni TLS (<https> saytlarda), SSH lar misolida amaliy ko'rinishini keltiramiz:

1. Client (browser) va server “salomlashadi”.

2. Sertifikat orqali serverning ochiq kalitini oladi.

3. Client tasodifiy sessiya kalitini shifrlab yuboradi.

4. Keyin: Har bir HTTP so'rov va javob AES bilan shifrlanadi yoki boshqa simmetrik algoritm.

Natijada:

• Wi-Fi tarmog'ini tinglayotgan odam faqat “bema'ni bitlar to'dasini” ko'radi.

• Login, parol, karta raqamlarining mazmunini o'qiy olmaydi.

SSH misolida esa,

• Client va server Diffie–Hellman kabi mexanizmlar bilan umumiy kalit kelishib oladi.

• Shundan keyin barcha buyruqlar, natijalar, fayl uzatishlar shifrlangan kanal orqali boradi.

• Siz `ssh user@server` qilganingizda, terayotgan buyruqlaringiz tarmoqdan ochiq ko'rinishda emas, shifrlangan ko'rinishda o'tadi.

Kriptografik protokollarda ma'lumotlar maxfiyligini buzilishiga olib keladigan asosiy omillar nafaqat matematik algoritmlarning murakkabligiga, balki tizimning dizayni, implementatsiyasi va sozlamalariga ham bog'liqdir.

Maxfiylik (Confidentiality) – bu ma'lumotni faqat ruxsat etilgan tomonlar o'qiy olishi va begona shaxslar uning mazmunini tushuna olmasligini anglatadi. Ushbu xususiyatni buzadigan asosiy omillar va xavf-hatarlarni quyidagilarga ajratish mumkin:

1. Protokol Dizayni va Implementatsiyasidagi Xatolar

• Noto'g'ri loyihalanish: Kriptografik algoritmlar matematik jihatdan mustahkam bo'lsa-da, ularning protokol darajasida noto'g'ri qo'llanilishi zaifliklarni keltirib chiqaradi.

• Implementatsiya kamchiliklari: Dasturiy kodni yozish jarayonidagi xatolar yoki tizimni noto'g'ri sozlash (masalan, sertifikatlarni tekshirishdagi xatoliklar) maxfiylikka jiddiy putur yetkazadi.

- Eski protokollardan foydalanish: Xavfsizligi bugungi kunda kafolatlanmagan SSL 2.0, SSL 3.0 yoki TLS'ning eski versiyalarini ishlatish.

2. Kalitlar bilan Bog'liq Muammolar

- Kalit uzunligining yetarsizligi: Juda qisqa kalitlar (masalan, 40-bit yoki 56-bitli DES) zamonaviy hisoblash quvvatlari yordamida tezda buzilishi (brute-force) mumkin.

- Kalitlarni noto'g'ri saqlash va boshqarish: Maxfiy kalitlarning o'g'irlanishi yoki ularning ochiq (himoyalangan) holatda saqlanishi butun tizimning buzilishiga olib keladi.

- Kalit taqsimoti muammosi: Kalitlar foydalanuvchilar o'rtasida xavfsiz kanallar orqali uzatilmasa, hujumchi ularni qo'lga kiritishi mumkin.

- Zaif parollar: Agar shifrlash kaliti foydalanuvchi tomonidan tanlangan zaif paroldan hosil qilingan bo'lsa, uni topish osonlashadi.

3. Shifrlash Rejimlari va Parametrlarining Noto'g'ri Tanlanishi

- Shifrlash rejimlari (Mode of Operation): Masalan, ECB (Electronic Code Book) rejimi bir xil ma'lumot bloklarini bir xil shifr-bloklarga aylantiradi, bu esa shifrlangan ma'lumotda ma'lum bir "naqsh" (pattern) qolishiga sabab bo'ladi.

- IV (Boshlang'ich vektor) va Nonce'ning qayta ishlatilishi: Agar IV yoki Nonce qiymatlari tasodifiy bo'lmasa yoki takrorlansa, hujumchi shifr oqimlarini analiz qilish orqali ochiq matnni tiklab olishi mumkin.

4. Maxfiylikka Qaratilgan Maxsus Hujum Turlari

- Man-in-the-Middle (MITM): Hujumchi ikki tomon o'rtasidagi aloqa kanaliga suqulib kirib, kalit almashinuv jarayonini nazorat qiladi yoki o'z kalitini o'rnatadi.

- Eavesdropping (Tinglash): Aloqa kanalini yashirincha tinglash orqali uzatilayotgan paketlarni to'plash.

- Yon kanalli (Side-channel) hujumlar: Tizimning ishlash vaqti, quvvat sarfi yoki elektromagnit nurlanishi kabi fizik ko'rsatkichlarini tahlil qilish orqali maxfiy ma'lumotlarni aniqlash.

- Matematik hujumlar: Masalan, RSA algoritmidagi modul yetarlicha katta bo'lmasa (≤ 1024 bit), uni tub ko'paytuvchilarga ajratish orqali yopiq kalitni hisoblab topish mumkin.

Maxfiylikni saqlash nafaqat kuchli algoritmlarni tanlashni, balki kalitlarni xavfsiz boshqarishni, zamonaviy protokollarni to'g'ri sozlashni va doimiy ravishda zaifliklarni tahlil qilib borishni talab etadi.

Kriptografik protokollarda maxfiylik (confidentiality) konsepsiyasi axborot xavfsizligining fundamental asoslaridan biri bo'lib, quyidagi nazariy va amaliy jihatlarni o'z ichiga oladi:

Maxfiylikning ta'rif va maqsadi

Maxfiylik — bu ma'lumotlarning faqat vakolatli (ruxsat berilgan) shaxslar tomonidan qabul qilinishi va o'qilishini ta'minlashdir. Uning asosiy maqsadi axborot almashinuvi jarayonida uchinchi tomonlarning (hujumchilarning) ma'lumot mazmunini anglashiga yo'l qo'ymaslik hisoblanadi. Bu konsepsiya zamonaviy kiberxavfsizlik infratuzilmasining asosiy ustunlaridan biri sifatida e'tirof etiladi.

Maxfiylikni ta'minlash mexanizmlari

Maxfiylikka asosan ma'lumotlarni shifrlash orqali erishiladi. Buning uchun quyidagi algoritmlar qo'llaniladi:

-Simmetrik shifrlash: Ma'lumotni shifrlash va deshifrlash uchun bir xil kalit ishlatiladi (masalan, AES). Bu usul juda tezkorligi bilan ajralib turadi.

-Asimmetrik shifrlash: Ochiq va yopiq kalitlar juftligidan foydalaniladi (masalan, RSA, ECC). U kalitlarni ochiq kanallar orqali xavfsiz almashish imkonini beradi.

-Gibrid tizimlar: Amaliyotda eng samarali model hisoblanib, bunda kalit almashinuvi asimmetrik usulda, asosiy ma'lumotlarni shifrlash esa simmetrik usulda amalga oshiriladi (masalan, TLS protokoli).

Tizimli yondashuv va arxitektura

Maxfiylik konsepsiyasi nafaqat oddiy shifrlash, balki axborot tizimlari arxitekturasining xavfsizlik asosini tashkil etuvchi tizimli mexanizmdir. U quyidagi murakkab jarayonlarni o'z ichiga oladi:

Kalitlarni boshqarish (Key Management): Kalitlarni xavfsiz yaratish, tarqatish va yangilash jarayonlari to'g'ri tashkil etilmasa, hatto eng kuchli shifrlash ham zaiflashib qoladi.

Protokollarning o'rni: TLS, IPsec va PGP kabi protokollar maxfiylikni ta'minlash bilan birga autentifikatsiya va ma'lumot butunligini ham birlashtirgan tizimli yechimlardir.

Kelajakdagi istiqbollar

Kvant kompyuterlarining rivojlanishi an'anaviy maxfiylik usullariga (masalan, RSA) tahdid solmoqda. Shu sababli, kelgusida yuqori darajadagi maxfiylikni ta'minlash uchun postkvant kriptografiya protokollari (masalan, CRYSTALS-Kyber) joriy etilishi strategik ahamiyat kasb etmoqda.

Kriptografik protokollarning funksional vazifalaridan ikkinchisi butunlik (integrity) vazifasi hisoblanadi. Bu funksional vazifa ma'lumot uzatish jarayonida o'zgartirilmaganini tasdiqlaydi. Hash-funksiyalar, MAC (Message Authentication Code) va raqamli imzo ishlatiladi. Butunlik – kriptografik protokollarning maxfiylikdan keyingi eng muhim funksiyalaridan biri.

Ta'rif: Butunlik – bu ma'lumot yo'lda o'zgarmagan bo'lishi, ya'ni jo'natilgan narsa aynan o'sha holatda qabul qilinishidir. Kimdir tarmoqdagi paketni ushlab, bitta bitini ham o'zgartirsa, qabul qiluvchi buni aniqlashi kerak. Aks holda hujumchi summa miqdorini, buyruq mazmunini, fayldagi ma'lumotni yashirincha o'zgartirib qo'yishi

mumkin. Shuning uchun kriptografik protokollar faqat shifrlash bilan cheklanmaydi, balki ma'lumotga "himoya kodi" ham qo'shadi.

Butunlik — bu axborotning uzatish yoki saqlash jarayonida o'zgarishsiz, asl holida qolishini ta'minlovchi xavfsizlik xususiyatidir. Uning asosiy maqsadi ma'lumotlarning ruxsatsiz o'zgartirilishi, tasodifiy buzilishi yoki hujumchi tomonidan soxtalashtirilishini oldini olish va aniqlashdan iborat. Butunlik vazifasi axborot xavfsizligining "to'rt ustunidan" biri bo'lib, u axborot tizimlarining ishonchliligini kafolatlaydi.

Kriptografik protokollarning funksional vazifalaridan biri bo'lgan Butunlik (Integrity) axborotning uzatish yoki saqlash jarayonida ruxsatsiz o'zgartirilmaganligini va asl holida qolganligini kafolatlaydi. Quyida ushbu vazifa va uning texnik jihatlari haqida ilmiy-mantiqiy tahlil taqdim etiladi:

Butunlikni ta'minlashning texnik mexanizmlari

Ma'lumotlar yaxlitligini tekshirish uchun matematik va kriptografik usullar majmui qo'llaniladi:

- Xesh-funksiyalar (SHA-2, SHA-3): Bu funksiyalar ixtiyoriy hajmdagi ma'lumotni qat'iy uzunlikdagi "raqamli barmoq izi"ga (digest) aylantiradi. Agar ma'lumotda hatto bitta bit o'zgarsa ham, xesh qiymati butunlay o'zgaradi, bu esa o'zgartirishni darhol aniqlash imkonini beradi.

- MAC (Message Authentication Code): Ma'lumotlarni autentifikatsiyalash kodi xesh-funksiyaga qo'shimcha ravishda maxfiy kalitdan foydalanadi. U ma'lumotning nafaqat butunligini, balki uning ma'lum bir kalitga ega bo'lgan yuboruvchi tomonidan yaratilganligini ham tasdiqlaydi.

- Raqamli imzo (ERI): Asimmetrik kriptografiyaga asoslangan bo'lib, ma'lumotning butunligini va yuboruvchining haqiqiylikini bir vaqtda ta'minlaydi. Ma'lumot o'zgartirilsa, raqamli imzo verifikatsiyadan o'tmaydi.

- AEAD (Authenticated Encryption with Associated Data): Bu mexanizm shifrlash va butunlikni tekshirishni bir vaqtda amalga oshiradi. Masalan, AES-GCM algoritmi ma'lumotni ham maxfiy saqlaydi, ham uning yaxlitligini kafolatlaydi.

Protokollarda butunlikka quyidagi omillar xavf soladi:

Xesh kolliziyasi: Ikki xil ma'lumot uchun bir xil xesh qiymatining hosil bo'lishi, bu hujumchiga ma'lumotni soxtalashtirish imkonini berishi mumkin.

Ma'lumotlarni almashtirish yoki o'zgartirish: Agar protokolda tegishli tekshiruvlar bo'lmasa, hujumchi paketlar mazmunini o'zgartirishi mumkin.

Qayta yuborish hujumi (Replay attack): Hujumchi haqiqiy ma'lumotni o'zgartirmagan holda uni qayta-qayta yuborib, tizimni chalg'itishi mumkin.

Butunlik vazifasi tizimli ravishda quyidagicha amalga oshiriladi:

TLS, IPsec va PGP: Ushbu protokollar shifrlash, autentifikatsiya va butunlikni ta'minlashni birlashtirgan tizimli yechimlar hisoblanadi. TLS protokolida ma'lumot almashinuvi jarayonida yaxlitlik MAC yoki AEAD rejimlari orqali tekshiriladi.

Nonce va Session ID: Har bir sessiya uchun unikallikni ta'minlab, avvalgi sessiya ma'lumotlarini qayta ishlatish orqali butunlikni buzishga qaratilgan hujumlarni oldini oladi.

Sequence Number: IPSec kabi protokollarda paketlar ketma-ketligini tekshirish orqali paketlarning tushib qolishi yoki o'rni almashishini nazorat qiladi.

Axborot xavfsizligining ustunlari bir-birini to'ldiradi, lekin farqli vazifalarni bajaradi:

Butunlik (Integrity) va Autentifikatsiya (Authentication): Butunlik ma'lumotning o'zgarmaganiga javob bersa, autentifikatsiya ma'lumotni yuborgan shaxsning kimligiga (haqiqiyligiga) javob beradi.

Butunlik va Inkori etib bo'lmazlik (Non-repudiation): Inkori etib bo'lmazlik yuboruvchining o'z harakatini keyinchalik rad eta olmasligini ta'minlaydi (buning uchun ERI va vaqt tamg'asi kerak). Butunlik esa faqat texnik jihatdan ma'lumotning yaxlitligini ko'rsatadi.

Kriptografik protokollarning to'rtta asosiy ustuni mavjud:

Maxfiylik (Confidentiality): Axborot faqat vakolatli shaxslar tomonidan o'qilishini ta'minlash (AES, RSA kabi shifrlash usullari orqali).

Autentifikatsiya (Authentication): Yuboruvchi va qabul qiluvchi shaxslarning haqiqiyligini tasdiqlash (PKI va sertifikatlash tizimlari orqali).

Inkori etib bo'lmazlik (Non-repudiation): Ma'lumot almashinuvi faktini huquqiy va texnik jihatdan tasdiqlash (ERI texnologiyasi orqali).

Xulosa qilib aytganda, butunlik vazifasi kriptografik protokollarning arxitekturaviy ustuni bo'lib, u boshqa xavfsizlik mexanizmlari bilan birgalikda raqamli muhitda ishonchli aloqani kafolatlaydi.

Umuman olganda, kriptografik protokollar zamonaviy kibermakonda (internet, elektron tijorat, mobil aloqa, bulutli hisoblash va boshqalar) xavfsizlikning fundamental asosini tashkil etadi.

FOYDALANILGAN ADABIYOTLAR:

1. **Stallings, W.** (2022). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson Education.
2. Kriptografiya va tarmoq xavfsizligining asosiy tamoyillari, protokollar va amaliy qo'llanilishi.
3. **Bishop, M.** (2019). *Introduction to Computer Security* (2nd ed.). Addison-Wesley.
4. Kompyuter xavfsizligining fundamental tushunchalari, autentifikatsiya, avtorizatsiya va himoya mexanizmlari.
5. **Goodfellow, I., Bengio, Y., & Courville, A.** (2016). *Deep Learning*. MIT Press.

6. Chuqur o'rganishning nazariy asoslari, neyron tarmoqlar va ularning amaliy tatbiqlari.
7. **Bishop, C. M.** (2006). *Pattern Recognition and Machine Learning*. Springer.
8. Mashina o'rganishi va naqshlarni aniqlashning matematik asoslari va algoritmlari.
9. **Anderson, R.** (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
10. Xavfsiz tizimlar loyihalash, kriptografik protokollar va ularning zaifliklari tahlili.
11. **Diffie, W., & Hellman, M. E.** (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
12. Asimmetrik kriptografiyaning ilmiy asoslari va kalit almashish protokollari.
13. **Rivest, R. L., Shamir, A., & Adleman, L.** (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126.
14. RSA algoritmi va raqamli imzolarning nazariy asoslari.
15. **Schneier, B.** (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). Wiley.
16. Kriptografik algoritmlar, protokollar va ularning dasturiy amalga oshirilishi.
17. **Kaufman, C., Perlman, R., & Speciner, M.** (2002). *Network Security: Private Communication in a Public World* (2nd ed.). Prentice Hall.
18. Tarmoq xavfsizligi, TLS/SSL, IPsec va boshqa kriptografik protokollar.
19. **McGrew, D., & Viega, J.** (2004). The Galois/Counter Mode of Operation (GCM). *NIST Modes of Operation*.
20. AES-GCM rejimi va AEAD (Authenticated Encryption with Associated Data) texnologiyasi.
21. **IEEE Xplore Digital Library.** (2020–2023). *Kriptografiya va axborot xavfsizligi bo'yicha ilmiy maqolalar*.
22. Zamonaviy tadqiqotlar, yangi hujum usullari va himoya mexanizmlari.
23. **ACM Digital Library.** (2018–2023). *Computer and Communications Security konferensiya materiallari*.
24. Sun'iy intellekt va mashina o'rganishi asosida kriptografik tizimlarni tahlil qilish usullari.
25. **SpringerLink.** (2019–2023). *Journal of Cryptology, Computers & Security*.
26. Kriptografik protokollar, zaifliklar tahlili va xavfsizlik mezonlari.
27. **National Institute of Standards and Technology (NIST).** (2020). *FIPS 140-3: Security Requirements for Cryptographic Modules*.
28. Kriptografik modullar uchun xavfsizlik standartlari va talablar.