**O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

“Kompyuter tarmoqlari” fanidan

**MUSTAQIL ISH**

**MAVZU:** Zamonaviy tarmoqlarda kriptogrofiya tamoyillari: Simmetrik kalit va ochiq kalit

**Topshirdi:** Turdiyev Muhammadqodir

**Qabul qildi:** Atadjanova Nozima

##### Toshkent 2024

Reja:

Kirish

Kriptografiya zamonaviy tarmoqlar tamoyillari. Asosiy qism

1.Kriptografiya-zamonaviy tarmoqlarni himoya qilishda hal qiluvch 2.Simmetrik kalit va ochiq kalit

3.Simmetrik kalit va ochiq kalit orasidagi farqi. Xulosa

KIRISH

Kriptografiyani dushmanlar yoki uchinchi shaxslar ishtirokida xavfsiz aloqa san'ati va ilmi sifatida ko'rish mumkin, ular xabar qilinayotgan ma'lumotni ushlab turish yoki manipulyatsiya qilishga urinishlari mumkin. U ochiq matnni (o'qilishi mumkin bo'lgan ma'lumotlarni) shifrlangan matnga (o'qilmaydigan ma'lumotlar) va aksincha, ruxsatsiz shaxslar tushunishi qiyin bo'lgan tarzda aylantirish uchun matematik algoritmlardan foydalanishni o'z ichiga oladi.

Kriptografiyaning asosiy maqsadlari maxfiylik, yaxlitlik, autentifikatsiya va rad etmaslikdir.

1. Maxfiylik: Kriptografiya faqat vakolatli shaxslarga yetkazilayotgan ma'lumotlarga kirishi va tushunishi uchun foydalaniladi. Bunga shifrlash orqali erishiladi, bu ma'lumotlarni shunday shifrlaydiki, uni faqat tegishli kalit yoki kalitlarga ega bo'lganlar tushunishi mumkin.
2. Yaxlitlik: Kriptografiya ma'lumot uzatish vaqtida o'zgartirilmagan yoki buzilmaganligini tekshirishga yordam beradi. Bunga ko'pincha dastlabki ma'lumotlarga kiritilgan o'zgarishlarni aniqlash uchun ishlatilishi mumkin bo'lgan kirish ma'lumotlaridan qat'iy o'lchamdagi belgilar qatorini (xesh qiymati) hosil qiluvchi kriptografik xesh funktsiyalaridan foydalanish orqali erishiladi.
3. Autentifikatsiya: Kriptografiya muloqot qiluvchi tomonlarning shaxsini tekshirish imkonini beradi. Bu xabarni jo'natuvchi yoki qabul qiluvchining o'zi da'vo qilgan shaxs ekanligini tasdiqlashga yordam beradi. Autentifikatsiya qilish uchun odatda ochiq kalit kriptografiyasiga asoslangan raqamli imzolardan foydalaniladi.
4. Rad etmaslik: jo'natuvchining ma'lum bir xabarni yuborganligini rad etishining oldini olish uchun kriptografik usullardan foydalanish mumkin. Raqamli imzolardan foydalangan holda, qabul qiluvchi xabarning kelib chiqishini isbotlashi mumkin va jo'natuvchi keyinchalik uni yuborganligini rad eta olmaydi.

Kriptografiya zamonaviy kiberxavfsizlikning muhim tarkibiy qismi bo'lib, xavfsiz aloqa protokollari, raqamli to'lovlar, ma'lumotlarni saqlash, kirishni boshqarish va identifikatsiyani boshqarish kabi keng doiradagi ilovalarda qo'llaniladi. Texnologiya taraqqiyotda davom etar ekan, kriptografiyada paydo bo'ladigan tahdidlarni bartaraf etish va raqamli ma'lumotlarning xavfsizligi va maxfiyligini ta'minlash uchun ishlatiladigan texnika va algoritmlar ham rivojlanmoqda.

Kriptografiya zamonaviy tarmoqlarda ma'lumotlarning xavfsizligi va maxfiyligini ta'minlashda hal qiluvchi rol o'ynaydi. Zamonaviy tarmoqlar kontekstida kriptografiyaning ba'zi asosiy tamoyillari:

1. Maxfiylik:
   * Ta'rif: Ma'lumot faqat uni ko'rish huquqiga ega bo'lganlar uchun ochiq bo'lishini ta'minlash.
   * Amalga kiritish: Shifrlash maxfiylikka erishishning keng tarqalgan usuli hisoblanadi. Bu algoritmlar va kalitlar yordamida ochiq matnli ma'lumotlarni xavfsiz, o'qilmaydigan formatga (shifrlangan matn) aylantirishni o'z ichiga oladi.
2. Yaxlitlik:
   * Ta'rif: Ma'lumot uzatish yoki saqlash vaqtida o'zgartirilmaganligini tekshirish.
   * Implementation: Xesh funksiyalari ko'pincha ma'lumotlar uchun qat'iy o'lchamdagi xesh qiymatini (dijest) yaratish uchun ishlatiladi. Ma'lumotlardagi har qanday o'zgarish boshqa xesh qiymatiga olib keladi va bu buzishni aniqlash imkonini beradi.
3. Autentifikatsiya:
   * Ta'rif: Muloqot qiluvchi tomonlarning shaxsini tekshirish.
   * Amalga kirish: Raqamli imzolar va sertifikatlar jo'natuvchi yoki qabul qiluvchining haqiqiyligini ta'minlashga yordam beradi. Ochiq kalitlar infratuzilmasi (PKI) odatda raqamli sertifikatlarni boshqarish uchun ishlatiladi.
4. Rad etmaslik:
   * Ta'rif: Tomon xabar yoki tranzaksiyaning haqiqiyligini inkor eta olmasligini ta'minlash.
   * Amalga kirish: Raqamli imzolar ham rad etmaslikka yordam beradi. Yuboruvchi elektron raqamli imzosi biriktirilgan bo'lsa, xabar yuborishni rad eta olmaydi.
5. Kalitlarni boshqarish:
   * Tanrif: Shifrlash, shifrni ochish va autentifikatsiya qilish uchun ishlatiladigan kriptografik kalitlarni xavfsiz boshqarish.
   * Amalga keltirish: Xavfsiz kalit almashish protokollaridan foydalanish, kalitlarni davriy aylantirish va kalitlarni xavfsiz saqlash samarali kalitlarni boshqarishning muhim komponentlari hisoblanadi.
6. Kirishni boshqarish:
   * Ta'rif: Oldindan belgilangan qoidalar va siyosatlar asosida maxfiy ma'lumotlarga kirishni cheklash.
   * Amalga oshirish: Kriptografik usullar kirishni boshqarish mexanizmlari bilan birgalikda faqat vakolatli shaxslar yoki tizimlar muayyan ma'lumotlarga kirishini ta'minlashga yordam beradi.
7. Xavfsiz aloqa protokollari:
   * Ta'rif: Ma'lumotlarni uzatishni ta'minlash uchun kriptografik usullarni o'z ichiga olgan protokollardan foydalanish.
   * Amalga keltirish: Misollar orasida veb-aloqa xavfsizligini ta'minlash uchun SSL/TLS va tarmoq darajasidagi aloqalarni ta'minlash uchun IPsec kiradi.
8. Tasodifiylik:
   * Ta'rif: Xavfsizlikni oshirish uchun kriptografik jarayonlarga tasodifiylikni joriy qilish.
   * Amalga keltirish: Tasodifiy raqamlar generatorlari kriptografik kalitlarni yaratish va ishga tushirish vektorlari kabi turli kriptografik ilovalarda qo'llaniladi.
9. Dizayn bo'yicha xavfsizlik:
   * Tanrif: Xavfsizlik choralarini boshidanoq tizimlarni loyihalash va rivojlantirishga integratsiyalash.
   * Amalga kiritish: Birinchi navbatda xavfsizlik nuqtai nazarini qabul qilish rivojlanishning dastlabki bosqichlarida potentsial zaifliklarni aniqlash va bartaraf etishga yordam beradi.
10. Doimiy monitoring va moslashish:
    * Ta'rif: Kriptografik tizimlar xavfsizligini muntazam ravishda kuzatib borish va paydo bo'ladigan tahdidlarga moslashish.
    * Amalga keltirish: Vaqti-vaqti bilan xavfsizlik auditlari, zaifliklarni baholash va so'nggi kriptografik yutuqlar va zaifliklar haqida xabardor bo'lish doimiy xavfsizlikka hissa qo'shadi.

Ushbu tamoyillarni birgalikda amalga oshirish zamonaviy tarmoqlarni turli tahdidlarga qarshi himoya qilish uchun mustahkam poydevor yaratadi. Yodda tutingki, kriptografiya sohasi dinamik va so'nggi o'zgarishlardan xabardor bo'lish mustahkam xavfsizlik choralarini saqlash uchun juda muhimdir.

Kriptografiya zamonaviy tarmoqlarni himoya qilishda hal qiluvchi rol o'ynaydi va kriptografik algoritmlarning ikkita asosiy turi simmetrik kalit va ochiq kalit (assimetrik) kriptografiyadir. Mana har birining printsiplari:

Simmetrik kalit kriptografiyasi:

1. Bir kalitdan foydalanish:
   * Key Shared: Muloqot qilayotgan ikkala tomon ham bitta maxfiy kalitga ega.
   * Shifrlash va shifrni hal qilish: Xuddi shu kalit shifrlash va shifrni ochish uchun ishlatiladi.
2. Kuchli tomonlari:
   * Effektivlik: Simmetrik kalit algoritmlari odatda tezroq va kamroq hisoblash resurslarini talab qiladi.
   * Mashqlanishi: Katta hajmdagi maʼlumotlar uchun samarali.
3. Qiyinchiliklar:
   * Kalitlarni taqsimlash: Asosiy muammo umumiy maxfiy kalitni xavfsiz tarqatish va boshqarishdir.
   * Kalit almashinuvi: Agar kalit buzilgan bo'lsa, ikkala aloqa tomon ham xavf ostida.
4. Umumiy algoritmlar:
   * AES (Kengaytirilgan shifrlash standarti): Simmetrik kalitlarni shifrlash uchun keng qo'llaniladi.
   * DES (Ma'lumotlarni shifrlash standarti): Asosan AES bilan almashtirilgan eski standart.

Ochiq kalit (assimetrik) kriptografiya:

1. Kalit juftliklari:
   * Ochiq kalit: Xavfsiz xabar yuborishni istagan har bir kishi tomonidan shifrlash uchun ishlatiladi.
   * Maxfiy kalit: Maxfiy saqlanadi va shifrni ochish uchun ishlatiladi. Shaxsiy kalitni faqat egasi biladi.
2. Shifrlash va shifrni hal qilish:
   * Ochiq kalit: Xabarni shifrlaydi.
   * Maxfiy kalit: Xabarning shifrini ochadi.
3. Kuchli tomonlari:
   * Kalitlarni taqsimlash: Xavfsiz kalit almashinuviga ehtiyojni yo'q qiladi, chunki har bir foydalanuvchi umumiy/maxfiy kalit juftligiga ega.
   * Digital Signatures: Autentifikatsiya qilish uchun raqamli imzolarni yaratish imkonini beradi.
4. Qiyinchiliklar:
   * Hisoblash intensivligi: Asimmetrik algoritmlar odatda simmetrik algoritmlarga qaraganda sekinroq, shuning uchun ular ko'pincha kombinatsiyalangan holda qo'llaniladi.
5. Umumiy algoritmlar:
   * RSA (Rivest–Shamir–Adleman): Xavfsiz maʼlumotlarni uzatish uchun keng qoʻllaniladi.
   * Eliptik egri kriptografiya (ECC): RSA bilan solishtirganda kalitlarni yaratishda samaradorligi va kichikroq kalit o'lchamlari bilan mashhur.

Gibrid kriptotizimlar:

* Kuchli tomonlarini birlashtirish: Ko'pgina zamonaviy tizimlar simmetrik va assimetrik kriptografiya kombinatsiyasidan foydalanadi.
* Kalit almashinuvi: Assimetrik shifrlash ko'pincha xavfsiz kalit almashinuvi uchun ishlatiladi, nosimmetrik shifrlash esa haqiqiy ma'lumotlarni uzatish uchun ishlatiladi.

Kalitlarni boshqarish:

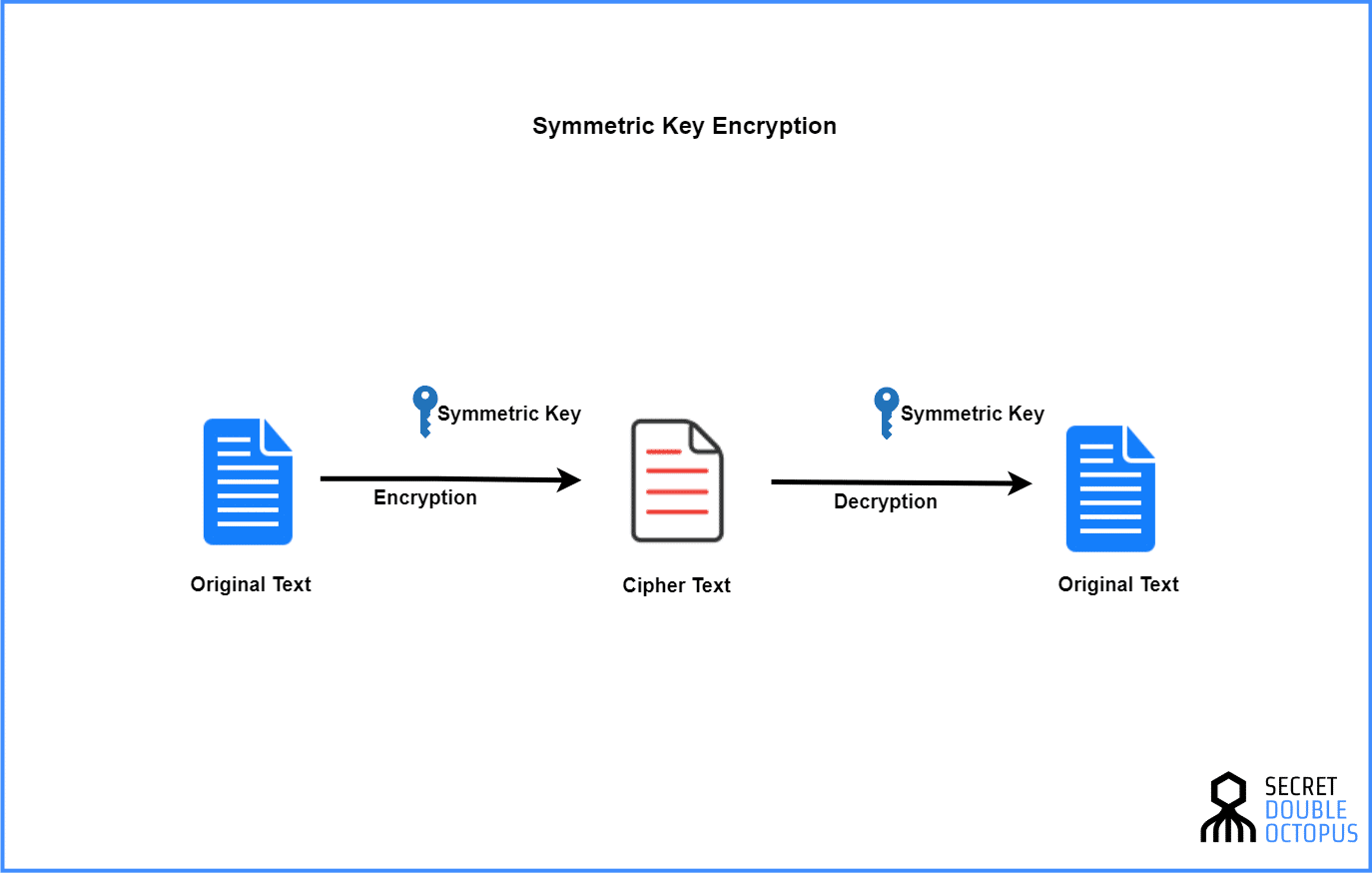
* Xavfsiz saqlash: Ham simmetrik, ham shaxsiy kalitlar xavfsiz tarzda saqlanishi kerak.
* Burish va yangilash: Xavfsizlikni oshirish uchun kalitlarni muntazam yangilash va o'zgartirish.

Kriptografiya, ma'lumotlar himoyalash sohasidagi keng qo'llaniladigan prinsiplardan biridir. Ushbu sohada iki asosiy kriptografiya turining roli katta: simmetrik kalit va ommaviy kalit.

1. Simmetrik Kalitlar:

Simmetrik kriptografiyada, xabar yuboruvchisi va qabul qiluvchisi bir xil kalitni (maxfiy so'zni) o'zlaridan foydalanadi. Ushbu kalitni bir paytda xabar yuboruvchisi va qabul qiluvchisi o'rtasida amalga oshirish zarur. Bu usul yaxshi xatolarni kamaytiradi, ammo kalitni xabar yuboruvchisiga xavfsiz tarzda yetkazib berish lozim.

Simmetrik kriptografiya misollaridan biri DES (Data Encryption Standard), AES (Advanced Encryption Standard) kabi algoritmlar bo'lishi mumkin. Ular ma'lumotlar uchun maxfiy so'zlar qo'shishda va ularga e'tibor qaratishda ishlatiladi.



1. Ommaviy Kalitlar (Asimmetrik Kalitlar):

Ommaviy kriptografiyada, har bir foydalanuvchi ikkita kalitga ega bo'ladi: maxfiy (shaxsiy) va ommaviy (umumiy) kalitlar. Maxfiy kalitni faqat foydalanuvchi biladi va uni saqlash vaqtida, ommaviy kalit esa barcha foydalanuvchilar tomonidan bilinadi.

Ommaviy kalitlar bilan amal qilishda, foydalanuvchilar xabar yuborish va qabul qilish uchun ikkita kalitni o'zlarining o'zi generatsiya qiladi. Yuboruvchi foydalanuvchi xabarni o'z maxfiy kaliti bilan shifrlaydi va qabul qiluvchi foydalanuvchi uni o'z ommaviy kaliti bilan yechadi.

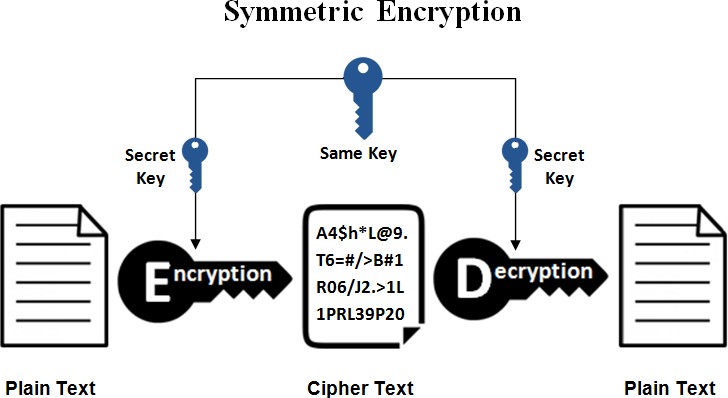
RSA (Rivest-Shamir-Adleman) va ECC (Elliptic Curve Cryptography) ommaviy kriptografiyaga oid mashhur algoritmlardan ba'zilari hisoblanadi.

Kriptografiya, xavfsizlikning asosiy qo'shimcha qismidir va maxfiylik, integritet va autentifikatsiya kabi tizimlarni ta'minlashda yordam beradi. Kriptografiya, shu bilan birga, internet, banklar, ma'lumot bazalari va boshqa ko'plab tarmoqlarda xavfsizlikni ta'minlashda ham keng qo'llaniladi.

XULOSA

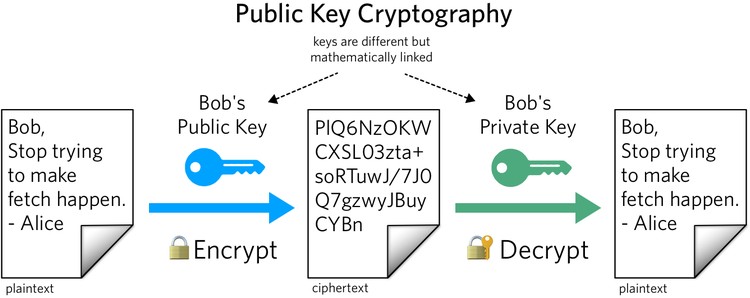
Kriptografiya, ma'lumotlar xavfsizligini ta'minlashda muhim rol o'ynaydi va hozirgi tarmoqlarda aniq usullar bilan amalga oshiriladi. Kriptografiyaning asosiy iki printsipi mavjud: simmetrik kalit (symmetric key) va ommalashtirilgan (jamlangan) kalit (public key). Mana bu ikkala printsipni o'zbek tilida qisqa xulosa:

1. Simmetrik Kalit (Symmetric Key):
   * Tushuncha: Bu usulda, ma'lumotni yuboruvchi va qabul qiluvchi tomonlar bir xil kalitni ishlatishadi.
   * Foydalanish: Ma'lumotni shifrlash va unshifrlashda bitta kalit ishlatiladi. Ushbu kalitni tanlagan holda, to'g'ridan-to'g'ri ma'lumot almashish mumkin.
   * Muhimiyat: Bu usul odatda tez va samarali bo'lib, katta miqdordagi ma'lumotlarni shifrlashda qulaylik yaratadi. Ammo, muammo shundaki, kalitni xavfsiz tarzda uzatish va uni tanlashda muammolar paydo bo'lishi mumkin.



1. Ommalashtirilgan Kalit (Public Key):

* Tushuncha: Bu usulda, ikki turdagi kalit ishlatiladi - ommalashtirilgan kalit va maxfiy kalit. Ommalashtirilgan kalitni foydalanuvchilar o'zlarining doimiy manziliga taqdim etishadilar, maxfiy kalit esa faqat ularga xos. Ommalashtirilgan kalit orqali yuborilgan ma'lumot maxfiy kalit bilan shifrlanadi va faqat maxfiy kalit orqali unshifrlanadi.
* Foydalanish: Xavfsiz bog'lanish va maxfiylikni ta'minlashda ishlatiladi. Masalan, veb-saytlar, elektron pochta va boshqa tarmoqlarda amal qiladi.
* Muhimiyat: Bu usul maxfiylikni oshiradi, chunki ommalashtirilgan kalitni tanlash shaxsiy ma'lumotlarni himoyalash uchun juda qulaydir. Ammo, usulning tezligi va energetika sarfiyoti yuqori bo'lishi mumkin.



Kriptografiya, hozirgi tarmoqlar va internet dunyosidagi axborot almashuvi va xavfsizlikni ta'minlashda asosiy qo'llanmalaridan biridir. Bu printsiplar yordamida ma'lumotlar xavfsiz tarzda almashish, saqlash va o'zaro almashuvi amalga oshiriladi.

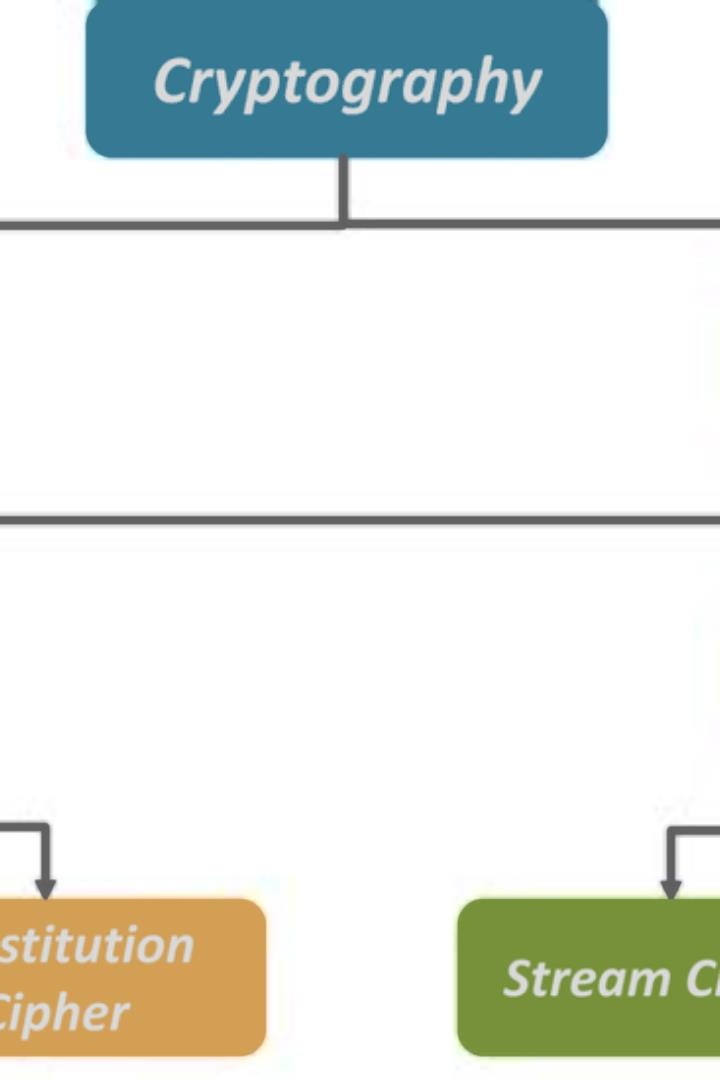
Zamonaviy tarmoqlarda ushbu kriptografik tamoyillarning kombinatsiyasi ko'pincha xavfsiz va samarali aloqa kanallarini yaratish uchun qo'llaniladi. Simmetrik kriptografiya tezlik va samaradorlikni ta'minlaydi, assimetrik kriptografiya esa asosiy tarqatish muammolarini hal qiladi va jamoat muhitida xavfsiz aloqani ta'minlaydi.

##### Foydalanilgan adabiyotlar va saytlar:

1. Cryptography and Network Security: Principles and Practice 2.Modern Cryptography

Applied Mathematics for Encryption and Information Security 3.Cryptography and Network Security

Principles and Practice, Global Ed



# Zamonaviy tarmoqlarda kriptografiya tamoillari: simmetrik kalit va ochiq kalit

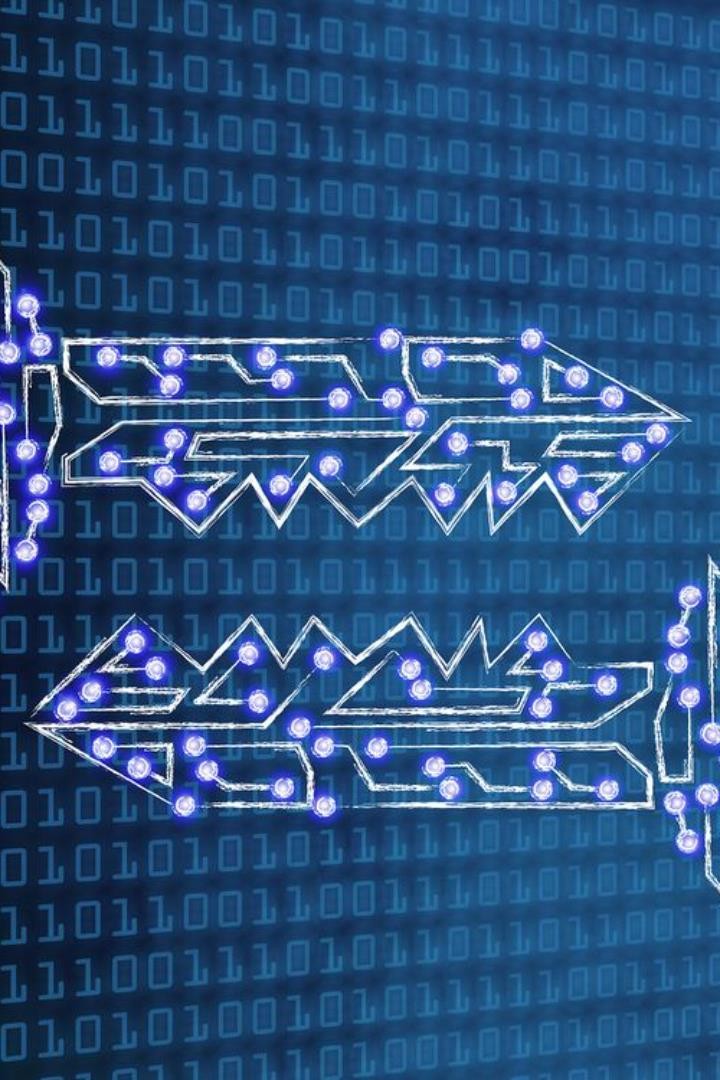
Ushbu taqdimotda biz hozirgi zamon tarmoqlarida kriptografiyaning ahamiyatini, shu jumladan asosiy tushunchalarni, kriptografik algoritmlarning turlarini, kriptografiyani amalga oshirishda qiyinchiliklarni tadqiq qilamiz.



# Kirish

Zamonaviy tarmoqlar orqali uzatiladigan axborotlarning xavfsizligi va maxfiyligini

ta'minlashda kriptografiya juda muhim rol o'ynaydi. Keling, kriptografiya olamiga sho'ng'ish va bugungi raqamli landshaftda uning ahamiyatini kashf qilaylik.



**Kriptografiya**

Kriptografiyaningajoyib dunyosiga xush kelibsiz, u erda sirlar aniqlanmaydigan kodlarga aylantiriladi, axborotni himoya qiladi va maxfiylikni ta'minlaydi.

# Shifrlarning turlari

### Almashtirish shifrlari

Har bir harfni boshqasiga almashtiring, masalan mashhur Sezar shifr.

### Transpozitsiyali shifrlar

Temir yo'l devori shifriga o'xshab, harflar tartibini ma'lum bir namunaga muvofiq qayta tartibga

soling.

### Bir martalikpad

Xabarning o'zigacha bo'lgan bir martalik kalitdan foydalanib, mukammal maxfiylikni ta'minlasin.

### Shifrlarni bloklash

Ma'lumotlarning kichik bo'laklarida ishlash, ularni

simmetrik kalit yordamida mustaqil ravishda

shifrlash.

# Simmetrik- kalit shifrlash

### Umumiy maxfiy kalit



Xabarni shifrlash va parolni shifrlash uchun jo'natuvchi ham, qabul qiluvchi ham bir xil maxfiy kalitdan foydalanadi.

### Samaradorlik

Simmetrik shifrlash jarayoni tez va kamroq hisoblash kuchini talab qiladi.

### Maxfiylik

Shifrlangan xabarga faqat vakolatli taraflarning kirishini ta'minlaydi.

# Asimetrik- kalit shifrlash

### Kalit juftligi

Ommaviy kalit shifrlashi mumkin bo'lgan va shaxsiy kalit shifrlashi mumkin bo'lgan ommaviy-xususiy kalit juftligini yarating.

### Xavfsiz aloqa

Shifrlangan xabarni qabul qiluvchining ochiq kalitidan foydalanib yuboring va uni shaxsiy kalit bilan

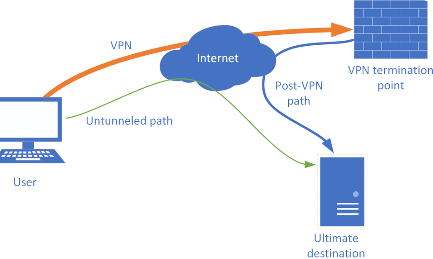
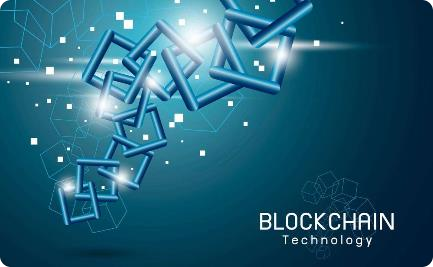
shifrlash.

### Avtorizatsiya

Yuboruvchining shaxsini tekshirish va uzatish vaqtida xolislikni ta'minlash uchun raqamli imzolardan foydalanish.

# Kriptografik protokollar

### Blokcheyn



Xavfsiz operatsiyalarni ta'minlash uchun markazlashtirilmasligi va taqsimlangan konsensus

mexanizmlaridan foydalanish.

### SSL/TLS

Ma'lumotlar maxfiyligi va yaxlitligini ta'minlovchi veb-ilovalar o'rtasida xavfsiz sessiyalar o'rnating.

**VPN**

Shifrlangan tunnel yaratish, ommaviy tarmoqlar orqali ma'lumotlar uzatishni himoya qilish.

# Kriptografiyaningqo'llanmalari

### 1 Xavfsiz aloqa

Onlayn o'zaro ta'sirlar davomida maxfiyligini va sezgir ma'lumotlarning maxfiyligini ta'minlash.

### 3 Raqamli imzolar

**2 Ma'lumotlarni himoyaqilish**

Dam olish paytida ma'lumotlarni shifrlash va xavfsiz saqlash, ruxsatsiz kirishning oldini olish va yaxlitlikni saqlash.

Rad etmaslikni taʼminlagan holda elektron hujjatlarninghaqiqiyligi va xolisligini tekshirish.



**Kriptografiyaningmuammolari vakelajagi**



#### Kvanthisoblash

Potentsial ravishda hozirgi kriptografik algoritmlarni eskirib, yangi post-kvant echimlarini talab qilmoqda.

#### Xavfsiz kalitlar almashinuvi

Kalitlarni zaifliklarsiz almashishningsamarali protseduralarini ishlab chiqish.

#### Uzluksiz tadqiqotlar

Shifrlash rivojlanayotgan tahdidlar va rivojlanayotgan texnologiyalarga qadamqo'yishi kerak.

# Hozirgi zamon tarmoqlarida kriptografiya

### Kriptografiyaning tasnifi

Kriptografiya – axborotni o'qib bo'lmaydigan formatga aylantirish orqali qo'riqlash amaliyoti, shu tariqa uni ruxsatsiz kirishdan himoya qilish.

### Kriptografiyaning ahamiyati

Kriptografiya zamonaviy tarmoqlarda ma'lumotlar maxfiyligini, yaxlitligini va haqiqiyligini ta'minlaydi, zararli aktyorlarning sezgir ma'lumotlarini himoya qiladi.

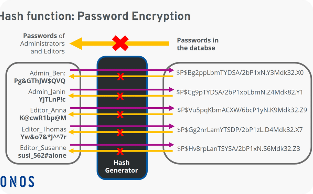
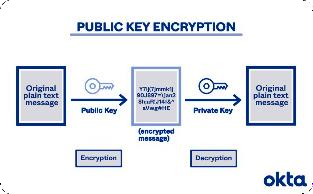
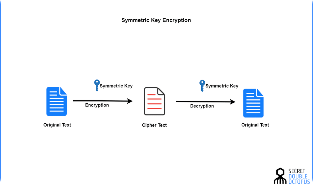


### Kriptografiyaning asosiy tushunchalari

Shifrlash, deshifrlash, kalit va algoritm kabi tushunchalarni tushunish hozirgi zamon tarmoqlarida kriptografiyaning asosini tashkil etadi.

# Kriptografik algoritmlarning turlari

### Simmetrik kalitlar kriptografiyasi



Shifrlash va shifrlash uchun bitta kalitdan foydalanishni o'z ichiga oladi. Bu samarali, ammo asosiy taqsimot qiyin bo'lishi mumkin.

### Ochiq kalitlar kriptografiyasi

Bir juft kalitdan foydalanadi - shifrlash uchun ochiq kalit va shifrlash uchun maxsus kalit. U kalit almashishga ehtiyoj bo'lmasdan xavfsiz aloqa kanallarini ta'minlaydi.

### Hash funksiyalari

Har qanday berilgan kirish uchun o'ziga xos sobit o'lchamdagi chiqish hosil qilish, xabar yaxlitligini ta'minlash va har qanday ruxsatsiz

o'zgarishlarni aniqlash.

### Raqamli imzolar

Raqamli xabar yoki hujjatning yaxlitligi va haqiqiyligini tekshiradigan shaxsni tasdiqlovchi mexanizm.

**Kriptografiyani zamonaviy tarmoqlarda qo'llash**

#### Ma'lumotlarni shifrlash

**1**

**2**

**3**

Uzatishdan oldin sezgir ma'lumotlarni shifrlash ruxsatsiz kirishni oldini oladi va maxfiylikni ta'minlaydi.

#### Xavfsiz aloqa

Ma'lumotlarni uzatish uchun xavfsiz kanallarni yaratish tinglash va o'rtadagi hujumlardan himoya qiladi.

#### Raqamli imzolar

Raqamli xabarlar yoki hujjatlarningkelib chiqishi va yaxlitligini tekshirish tavakkalchilikka asoslangan muhitni osonlashtiradi.

# Kriptografiyani takomillashtirishdagi qiyinchiliklar va omillar

**1 Kalitlarni boshqarish** Kriptografik kalitlarni tarqatish va xavfsiz saqlash

yirik tizimlarda sezilarli qiyinchilik tug'diradi.

1. **Ishlashta'siri** Kriptografik operatsiyalarninghisoblash

ustki qismi tarmoqlararo aloqa tezligi va samaradorligiga ta'sir ko'rsatishi mumkin.

1. **Algoritmikzaifliklar**

Kriptografik algoritmlarda uchraydigan zaifliklarni bartaraf etish uchun davriy tahlil va yangilanishlar talab etiladi.



# Simmetrikkalitlar kriptografiyasi. Tasnifi va misollar

Simmetrik kalitlar kriptografiyasi ham shifrlash, ham shifrlash uchun bir xil kalitdan foydalanadi. Simmetrik shifrlash tushunchasini o'rganingva haqiqiy dunyo misollarini kashf eting.

# Simmetrik kalit algoritmlari: turlari va

**foydalanish**

## DES (maʼlumotlarni shifrlash standarti) Name

Hozir ko'plab dasturlar uchun xavfli deb hisoblansa-da, keng tarqalgan simmetrik shifrlash algoritmi.

## AES (Kengaytirilgan shifrlash standarti)

DES o'rnini bosuvchi AES o'zining xavfsizligi va samaradorligi uchun keng qabul qilingan kuchli simmetrik shifrlash algoritmidir.



# O chiq kalitlar kriptografiyasi:

**tasnifi va namunalari**

Ommaviy kalit kriptografiya kalit juftligidan foydalanishni o'z ichiga oladi - shifrlash uchun ochiq kalit va shifrlash uchun shaxsiy kalit. Asimmetrik shifrlash kuchini kashf qilish.

# Asimmetrik kalit algoritmlari: turlari va

**foydalanish**

## RSA (Rivest-Shamir- Adleman)

Kalit almashish, raqamli imzolar va xavfsiz aloqa uchun mos bo'lgan keng tarqalgan assimetrik shifrlash algoritmi.

## ECC (Elliptik egri chiziqli kriptografiya)

Qisqa muddatli asosiy uzunlikdagi kuchli xavfsizlikni taklif qilib, ECC resurslar cheklangan muhitda tobora ommalashib bormoqda.

# Tarmoqxavfsizligi bo'yichaengyaxshi amaliyotlar

### 1 Kuchli maxfiy soʻzlar 🔒

Ruxsatsiz kirishni oldini olish uchun katta va kichik harflar, raqamlar va maxsus belgilar aralashmasi bilan murakkab parollar yaratish.

**3 îavŅsÒzÕÒÔŇÑvorÒÖ uhoŅazasÒ**🛡️ Kirish va chiquvchi tarmoq trafigini kuzatib borish, zararli bo'lishi mumkin bo'lgan

ulanishlarni filtrlash uchun xavfsizlik devorini amalga oshiring.

### 2 Doimiydasturiy ta'minot yangilanishlari 📲

Zaifliklarni yamash va so'nggi xavfsizlik tahdidlaridan himoya qilish uchun qurilmalaringiz va dasturiy ta'minotingizni yangilab turing.

### 4 Xodimlarningxavfsizligi bo'yicha trening🎓

Xodimlaringizni fishingelektron pochta xabarlarini aniqlash va shubhali veb-saytlardan qochish kabi tarmoq xavfsizligi bo'yicha eng yaxshi amaliyotlar bo'yicha o'rgating.

# Tarmoqxavfsizligi vositalari va texnologiyalari

## Kirishni aniqlash tizimlari (IDS)

Zararli faoliyat uchun tarmoqingizni kuzatib boringva xavfsizlikning har qanday buzilishi to'g'risida xabardor qiling.

## Vi rtual sha xsiy tarmoq

**(**In**V**te**P**rn**N**et**)**orqali xavfsiz

ulanishlarni o'rnating, ma'lumotlaringizni to'sib qo'yishdan va maxfiylikni ta'minlashdan himoya qiling.

## Xavfsizlik ma'lumotlari va hodisalarni boshqarish (SIEM)

Xavfsizlik hodisalarini real vaqt rejimida aniqlash va ularga javob berish uchun turli manbalardan ma'lumotlarni to'plash, tahlil qilish va korrelyatsiya qilish.

## Ikki faktorli autentifikatsiya (2FA)

Foydalanuvchilardan parol va o'ziga xos kod kabi ikkita identifikatsiya shaklini taqdim etishni talab qilib, qo'shimcha xavfsizlik qatlamini qo'shing.

# Simsiz tarmoqni himoyalash



### W Ĩ A 2 yoÔÒWPA3s hi frlashni yoqish

Ruxsatsiz kirishni oldini olish uchun kuchli shifrlash bilan Wi-Fi tarmog'ingizni himoya

qiling.

### Andozarouter maxfiy soʻzlarini oʻzgartirish

Hujumchilarningtarmoqingizga osongina kirishiga yo'l qo'ymaslik uchun yo'lovchining kirish ma'lumotlarini o'zgartiring.

### MAC manzillarni filtrlashni amalgaoshirish

Faqat oldindan tasdiqlangan MAC manzillariga ega bo'lgan muayyan qurilmalarga

simsiz tarmog'ingizga ulanishga ruxsat bering.



# Xulosa

Kriptografiya - bu zamonaviy tarmoqlarning ajralmas tarkibiy qismi bo'lib,

ma'lumotlarni himoya qilish, xavfsiz aloqani ta'minlash va raqamli

tranzaktsiyalarning yaxlitligini ta'minlash. Kriptografiya tamoyillari va usullarini tushunish orqali biz yanada xavfsiz va ishonchli raqamli dunyoni qurishimiz mumkin.