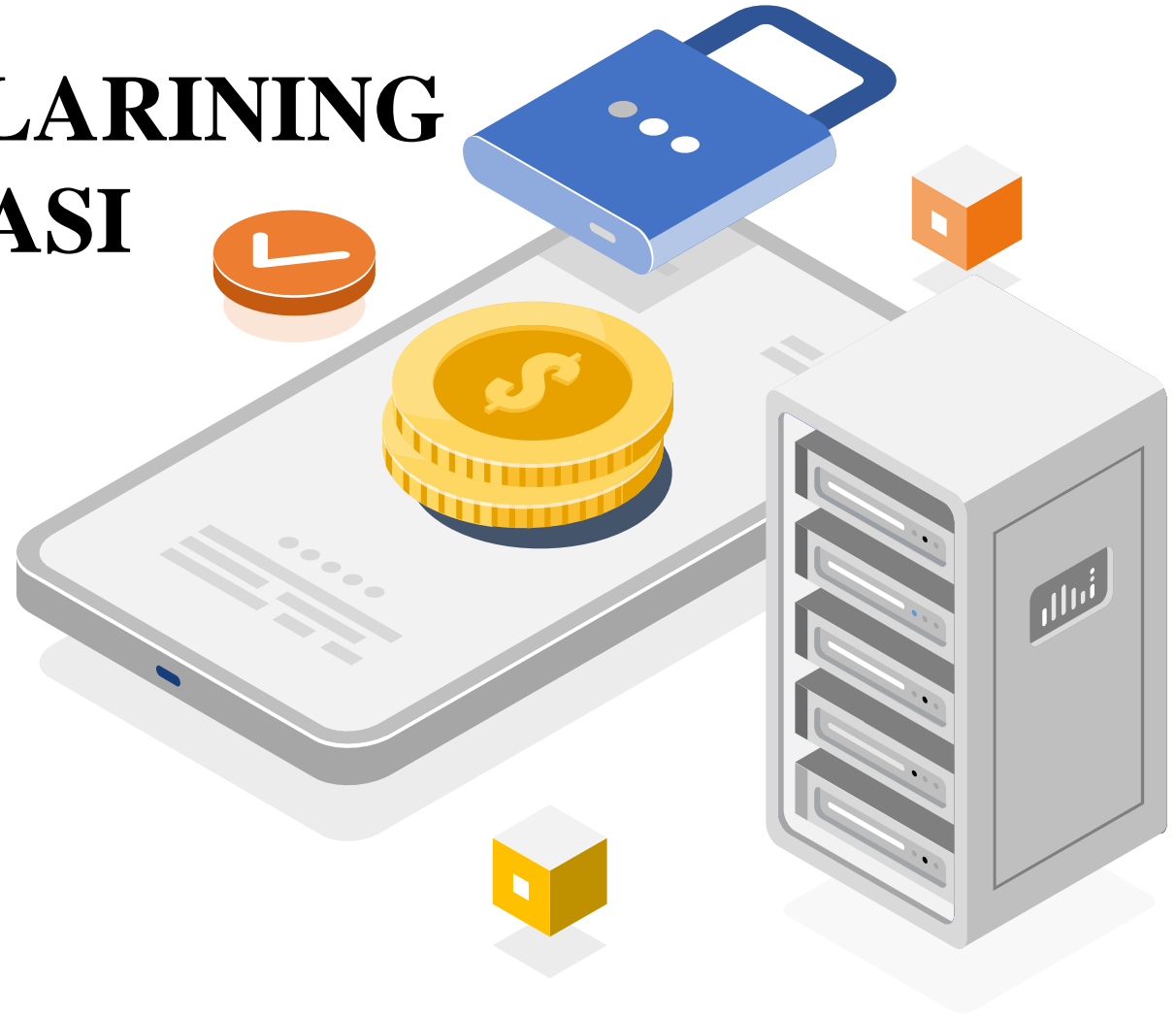


SHIFRLASH ALGORITMLARINING KLASSIFIKATSIYASI



Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo'yiladi:

- ❖ yetarli darajada kriptomustahkamlik;
- ❖ shifrlash va qaytarish jarayonining oddiyligi;
- ❖ axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi;
- ❖ shifrlashdagi kichik xatolarga ta'sirchan bo'lmasligi.

Ushbu talablarga quyidagi tizimlar javob beradi:

- ❖ o'rinlarini almashtirish;
- ❖ almashtirish;
- ❖ gammalashtirish;
- ❖ analitik o'zgartirish.

O‘rinlarini almashtirish shifrlash usuli bo‘yicha boshlang‘ich matn belgilarining matnning ma‘lum bir qismi doirasida maxsus qoidalar yordamida o‘rinlari almashtiriladi.

Almashtirish shifrlash usuli bo‘yicha boshlangich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtirilali.

Gammalashtirish usuli bo‘yicha boshlangich matn belgilari shifrlash gammasi belgilari, ya‘ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.

Tahliliy o‘zgartirish usuli bo‘yicha boshlang‘ich matn belgilari analitik formulalar yordamida o‘zgartiriladi, masalan, vektorni matritsaga ko‘paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo‘lsa, matritsa esa kalit sifatida xizmat qiladi.




Axborot jamiyatining shakllanishi bilan yirik davlatlar millionlab odamlarning umumiy nazoratining texnik vositalariga aylandi. Shu sababli, kriptografiya maxfiylik, ishonch, avtorizatsiya, elektron to'lovlar, korporativ xavfsizlik va boshqa muhim narsalarni ta'minlaydigan asosiy vositalardan biriga aylanmoqda.

Axborotni uning aylanishi orqali himoya qilish muammosi bilan shug'ullanadi *kriptologiya*, u ikki yo'nalishga bo'lingan: *kriptografiya* va *kriptoalyuta*. Ushbu sohalarning maqsadlari to'g'ridan-to'g'ri qarama-qarshi.

Kriptografiya axborotni o'zgartirishning matematik usullarini qidirish va tahqiq qilish bilan shug'ullanadi. *Kriptoalyuta*-kalitlarni bilmasdan ma'lumotlarning shifrlanishi mumkinligini o'rganish.



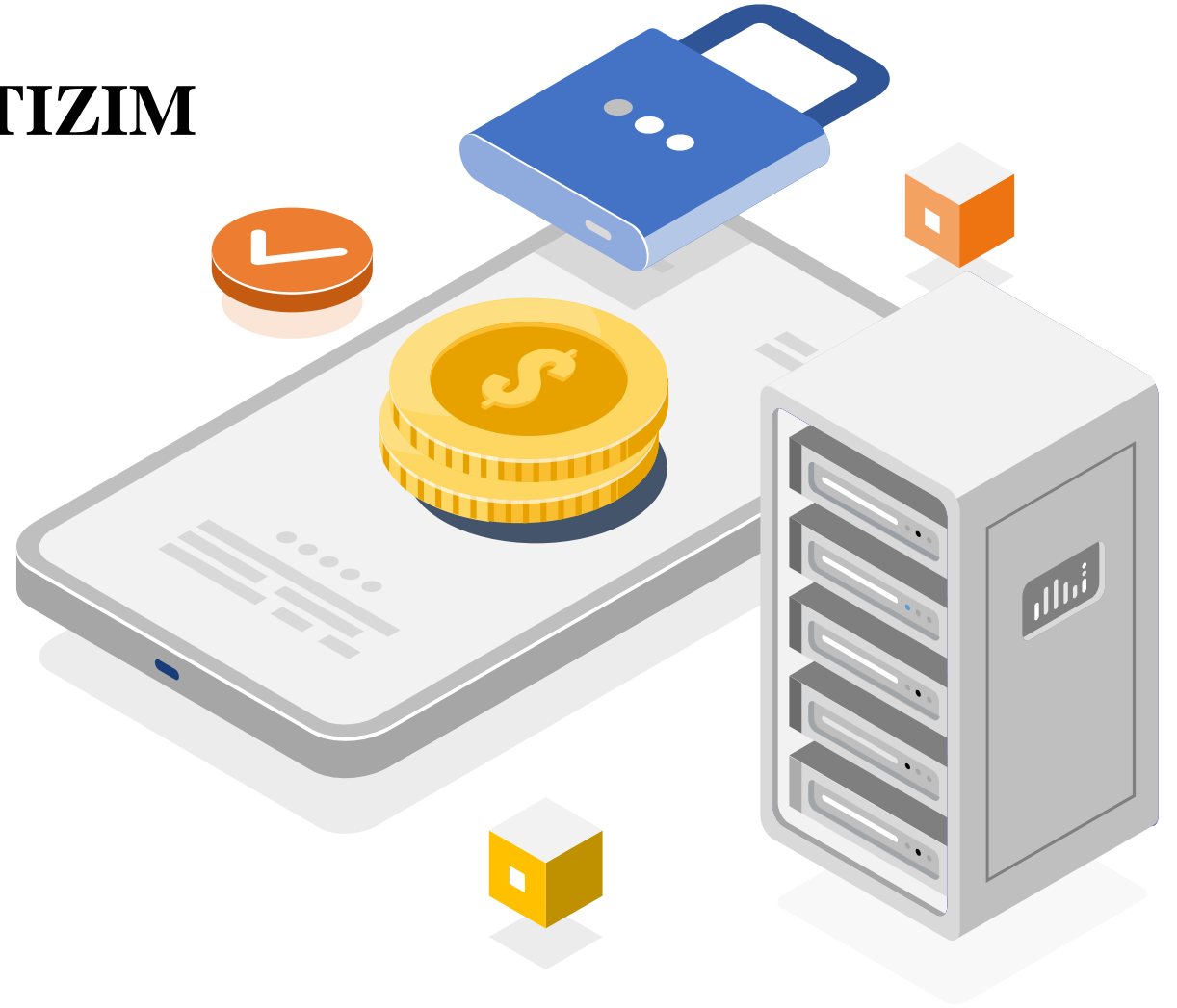
Zamonaviy kriptografiya 4 ta asosiy qismni o'z ichiga oladi:

-  **Simmetrik kriptosistemalar**
-  **Ochiq kalitlarning kriptotizimlari**
-  **Elektron imzo tizimlari**
-  **Kalitlarni boshqarish**

Maxfiy ma'lumotlarni aloqa kanallari orqali uzatish, uzatilayotgan xabarlarning autentifikatsiyasi va axborotni shifrlangan shaklda saqlash bu kriptografik usullardan foydalanishning asosiy yo'nalishlari hisoblanadi.

Kriptografiya ma'lumotlarni o'qishni (qayta tiklashni) faqat kalitni bilgan holda amalga oshiriladigan tarzda o'zgartiradi. Shifrlash va shifrlash zarur bo'lgan ma'lumot sifatida ba'zi alifboga asoslangan matnlar ko'rib chiqiladi.

SIMMETRİYALI KRIPTOTİZİM ASOSLARI



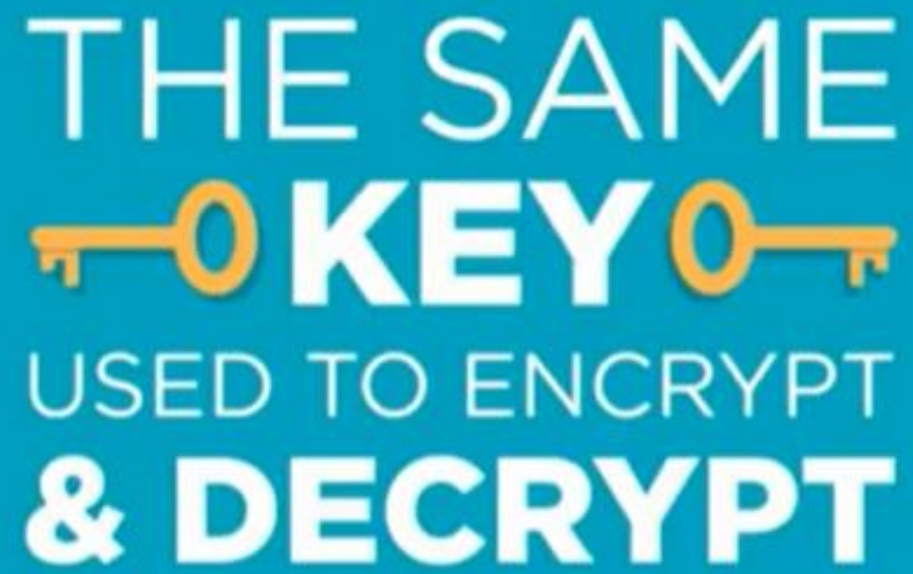




Hozirgi kunda kriptotizimni ikki sinfga ajratish mumkin:

- ☒ Simmetriyali bir kalitlilik (maxfiy kalitli)
- ☒ Asimmetriyali ikki kalitlilik (ochiq kalitli)

Simmetrik kriptotizimlar

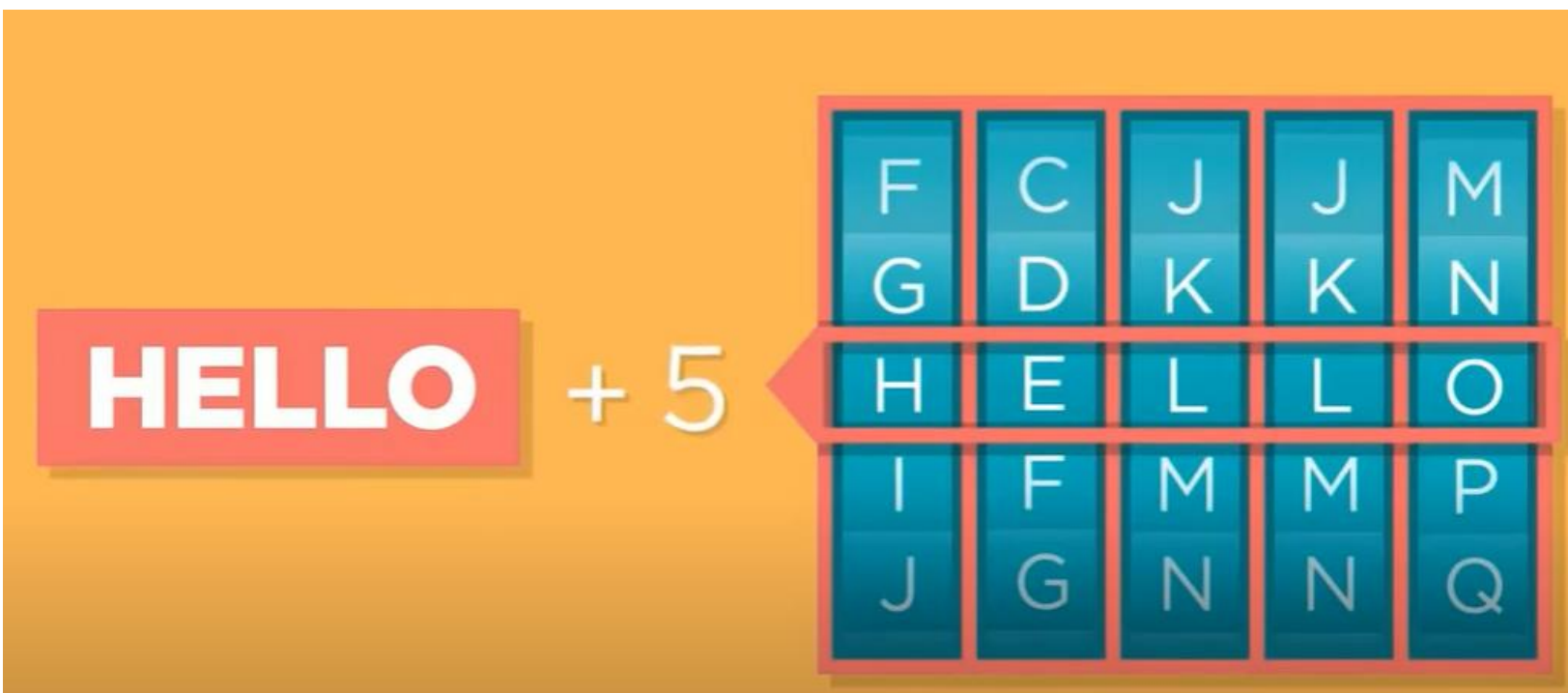
Bu shunday kriptoshifrlash tizimiki unda shifrlash ham deshifrlash ham aynan bir kalit yordamida amalga oshiriladi. Bu kriptotizim asimmetrik kriptotizimlar vujudga kelmasi turib faqatgina simmetrik tizimlardan foydalanilgan. Algoritmning kaliti o'zaro ma'lumotlar almashinayotgan tomonlarning har ikkalasi uchun ham boshqalardan sir saqlanishi kerak. Ma'lumotlarni qaysi simmetrik kriptotizim asosida shifrlanishi bu ikki tomon tomondan ma'lumot almashinishi oldin bajarish kerak



THE SAME
 **KEY** 
USED TO ENCRYPT
& **DECRYPT**

**SYMMETRIC
ENCRYPTION**





I	Q	K	E	P	N	A	F	C	N	Q	S	N	E	C	F	G	K	V	J	R	H	A
J	R	L	F	Q	O	B	G	D	O	R	T	O	F	D	G	H	L	W	K	S	I	B
K	S	M	G	R	P	C	H	E	P	S	U	P	G	E	H	I	M	X	L	T	J	C
L	T	N	H	S	Q	D	I	F	Q	T	V	Q	H	F	I	J	N	Y	M	U	K	D
M	U	O	I	T	R	E	J	G	R	U	W	R	I	G	J	K	O	Z	N	V	L	E
+5	+1	+8	+2	+2	+7	+3	+8	+4	+7	+5	+1	+8	+2	+2	+7	+3	+8	+4	+7	+5	+1	+8



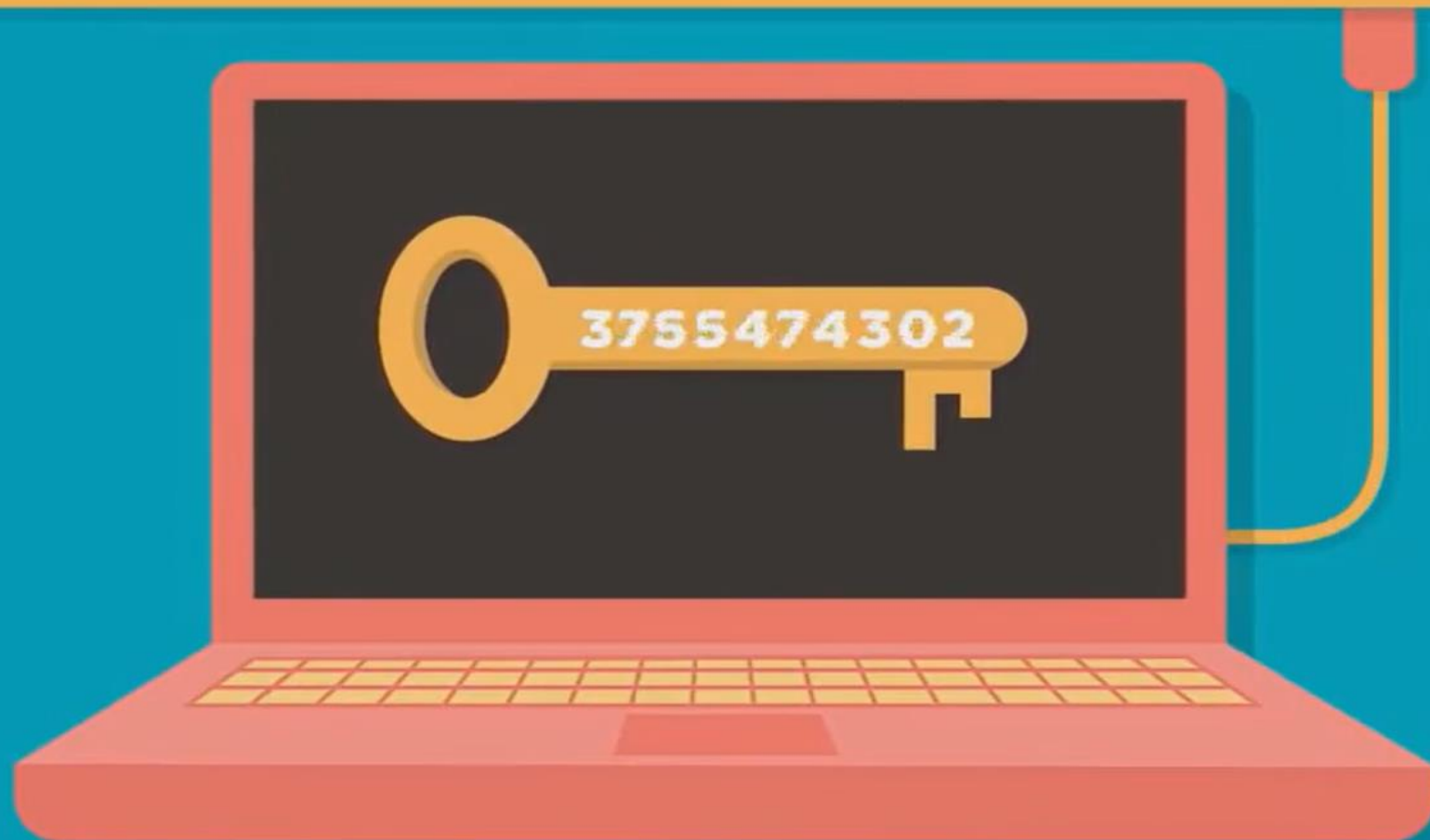
KSMG RPCHE PS UPG EHIMXLWJI

10 BILLION
POSSIBLE

SOLUTIONS



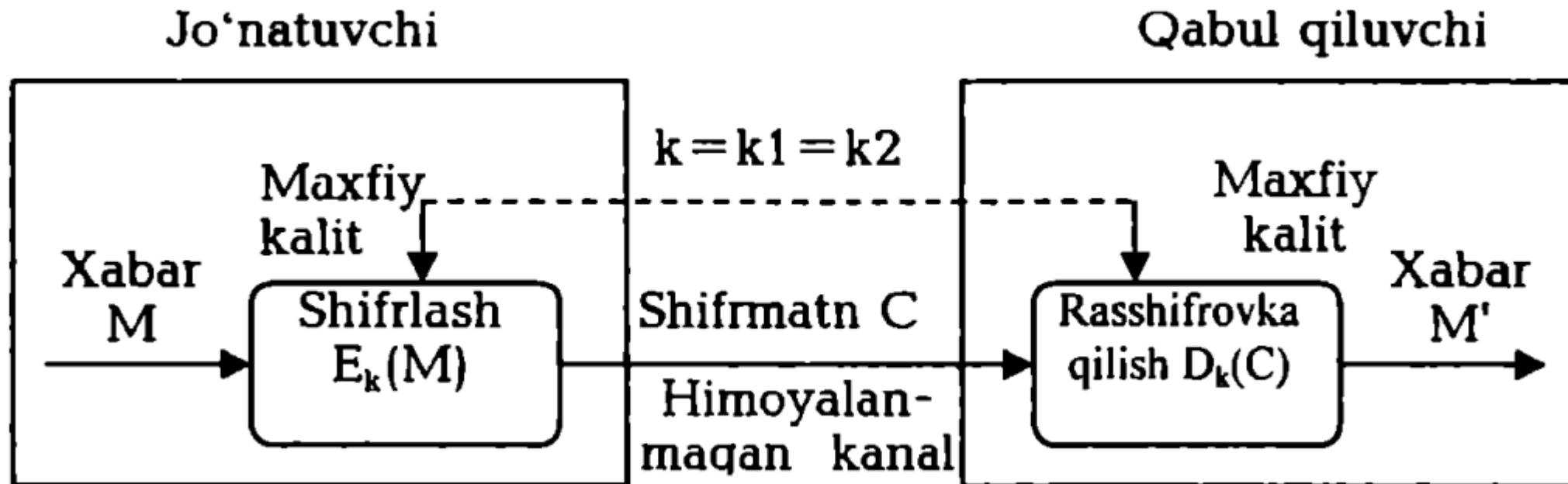
SAZJ OKMTI NU HBY YGSTFCRDX



256 BIT KEYS



Demak, shifrlash kalitidan foydalanish huquqiga ega bo'lgan har qanday odam axborotni rasshifrovka qilishi mumkin. Shu sababli, simmetrik kriptotizimlar maxfiy kalitli kriptotizimlar deb yuritiladi. Ya'ni shifrlash kalitidan faqat axborot atalgan odamgina foydalana olishi mumkin. Shifrlashning simmetrik kriptotizimi sxemasi 4.2-rasmda keltirilgan.




Simmetrik kriptotizimlarning turlar:

Simmetrik kriptotizimlarga quyidagi alqiritmlarni misol
qilib keltirishimiz mumkin:

- AES (Advanced Encryption Standart)
- DES (Data Encryption Standart)
- 3DES (Triple-DES)
- RC2 (Rivest shifri)
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA
- CAST

Simmetrik shifrlashning noqulayligi - axborot almashinuvi boshlanmasdan oldin barcha adresatlar bilan maxfiy kalitlar bilan ayirboshlash zaruriyatidir. Simmetrik kriptotizimda maxfiy kalitni aloqaning umumfoydalanuvchi kanallari orqali uzatish mumkin emas. Maxfiy kalit joʻnatuvchiga va qabul qiluvchiga kalitlar tarqatiluvchi himoyalangan kanallar orqali uzatilishi kerak.

ASYMMETRIC ENCRYPTION

DIFFERENT
 **KEYS** 
FOR ENCRYPTING
& **DECRYPTING**

Asimmetrik shifrlash ta'rifi

Asimmetrik shifrlash - bu shifrlash va parolni hal qilish uchun juft kalit (shaxsiy kalit va ochiq kalit) dan foydalanadigan shifrlash texnikasi. Asimmetrik shifrlashda xabarni shifrlash uchun ochiq kalit va xabarning parolini ochish uchun shaxsiy kalit ishlatiladi.

Xabarni yuborishdan manfaatdor bo'lgan har bir kishi uchun ochiq kalit ochiqdir. Shaxsiy kalit xabarni qabul qiluvchida sir saqlanadi. Ochiq kalit va algoritm bilan shifrlangan har qanday xabar bir xil algoritm va tegishli ochiq kalitning mos keladigan shaxsiy kalitidan foydalanib parolini ochadi. Asimmetrik shifrlash algoritmining bajarilishi sust. Asimmetrik shifrlash algoritmi tabiatan murakkab va yuqori hisoblash yukiga ega.

Asimmetrik shifrlash odatda internet kabi xavfsiz bo'lmagan vosita orqali xavfsiz kanalni yaratish uchun ishlatiladi. Asimmetrik shifrlash algoritmi eng keng tarqalgan **Diffie-Hellman** va **RSA** algoritmi.



PUBLIC KEY

SHARED WITH EVERYBODY

SO

ANYBODY CAN ENCRYPT A MESSAGE

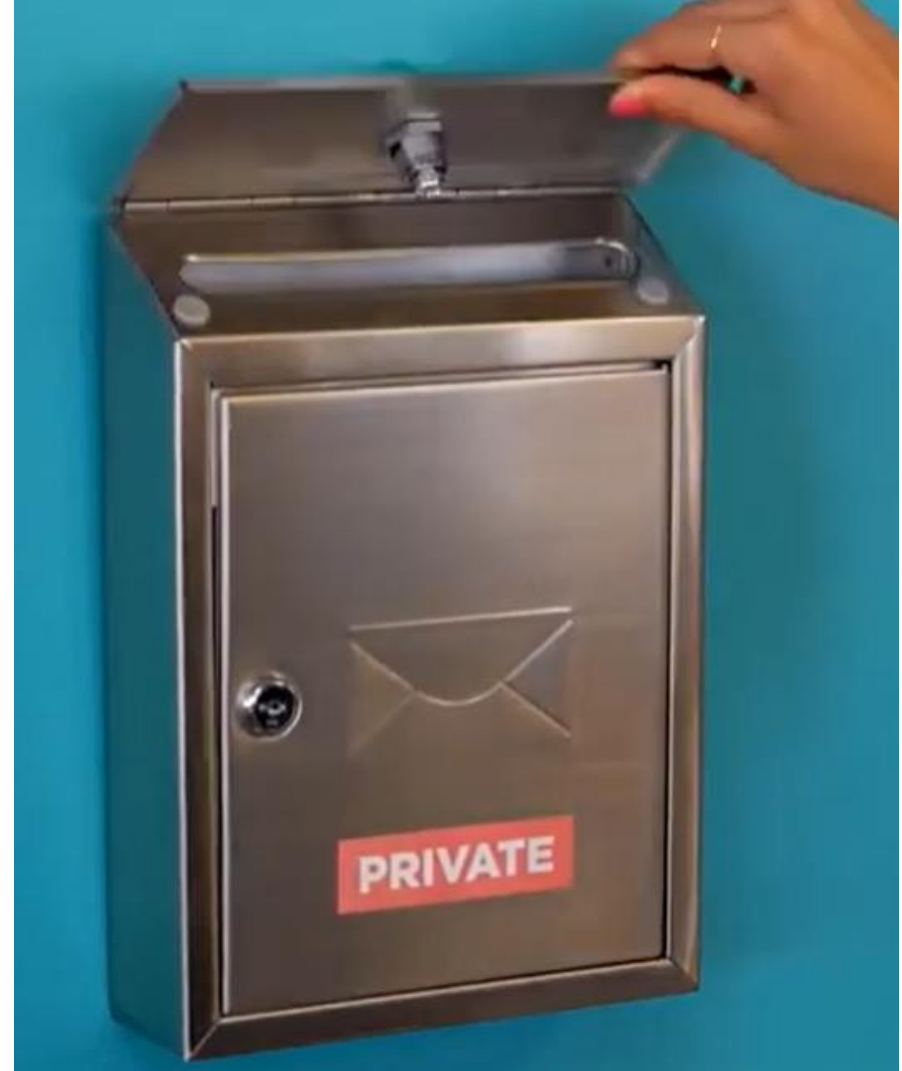
PRIVATE KEY

CAN ONLY BE DECRYPTED

BY

A COMPUTER WITH ACCESS









Login | HEMIS OTM axborot tizi



Новая вкладка



<https://hemis.samdu.uz/dashboard/login>

Taqqoslash jadvali

Taqqoslash uchun asos	Simmetrik shifrlash	Asimmetrik shifrlash
Asosiy	Simmetrik shifrlashda ham shifrlash, ham shifrlash uchun bitta kalit ishlatiladi.	Asimmetrik shifrlashda shifrlash va parolni hal qilish uchun boshqa kalit ishlatiladi.
Ishlash	Simmetrik shifrlash tez bajariladi.	Asimmetrik shifrlash yuqori hisoblash yuki tufayli sekin bajariladi.
Algoritmlar	DES, 3DES, AES va RC4.	Diffie-Xellman, RSA.
Maqsad	Nosimmetrik shifrlash ommaviy ma'lumotlarni uzatish uchun ishlatiladi.	Asimmetrik shifrlash ko'pincha maxfiy kalitlarni xavfsiz almashtirish uchun ishlatiladi.

Mustaqil ta'lim savollari

1. Kriptologiya nima va necha qismga bo'lingan?
2. Zamonaviy kriptografiya necha qismdan tashkil topgan?
3. Simmetriyali bir kalitlilik (maxfiy kalitli) nima?
4. Asimmetriyali ikki kalitlilik (ochiq kalitli)?
5. Simmetrik kriptotizim algoritmlariga misollar keltiring?
6. Simmetrik kriptotizimning kamchiligi nimada?
7. Asimmetrik va simmetrik kriptotizim farqlari?
8. Asimmetriyali shifrlash algoritmiga misollar keltiring
9. Kriptografiya himoyasida shifrlarga nisbatan talablarga qaysi tizimlar javob beradi?
10. Tahliliy o'zgartirish usuli