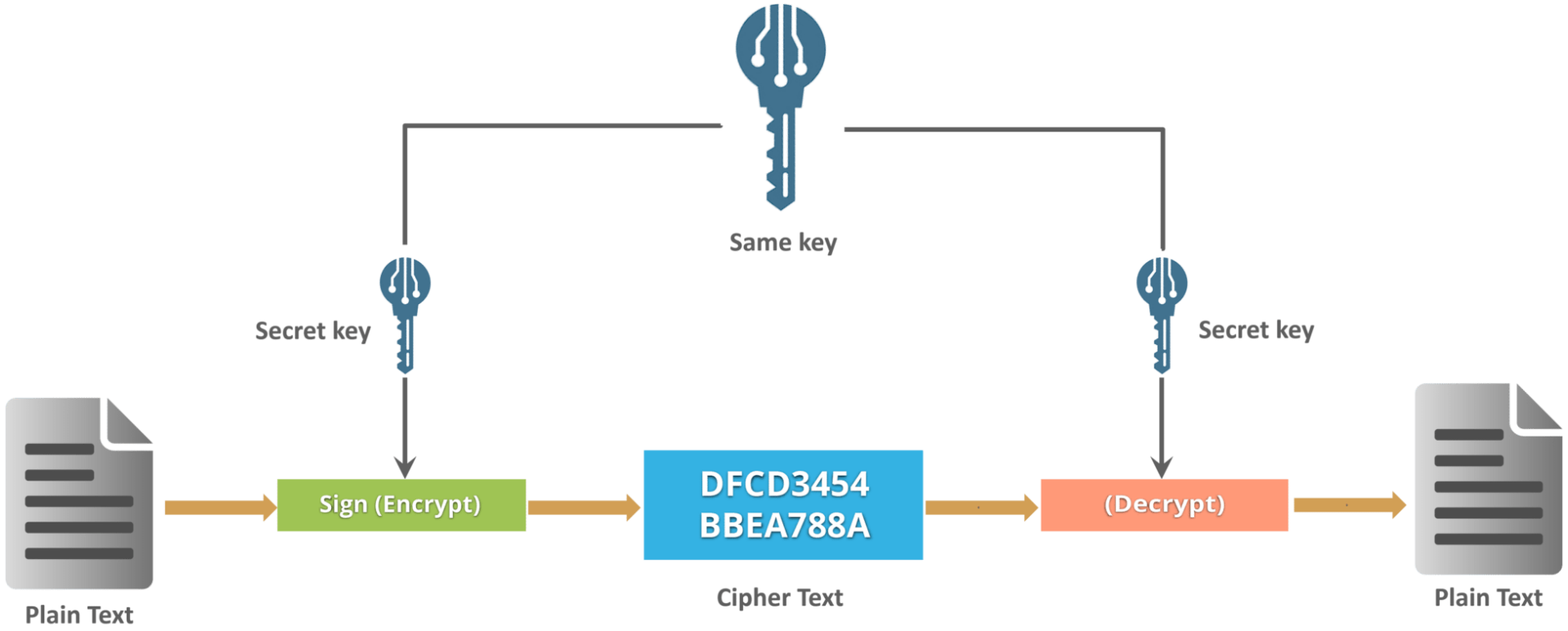
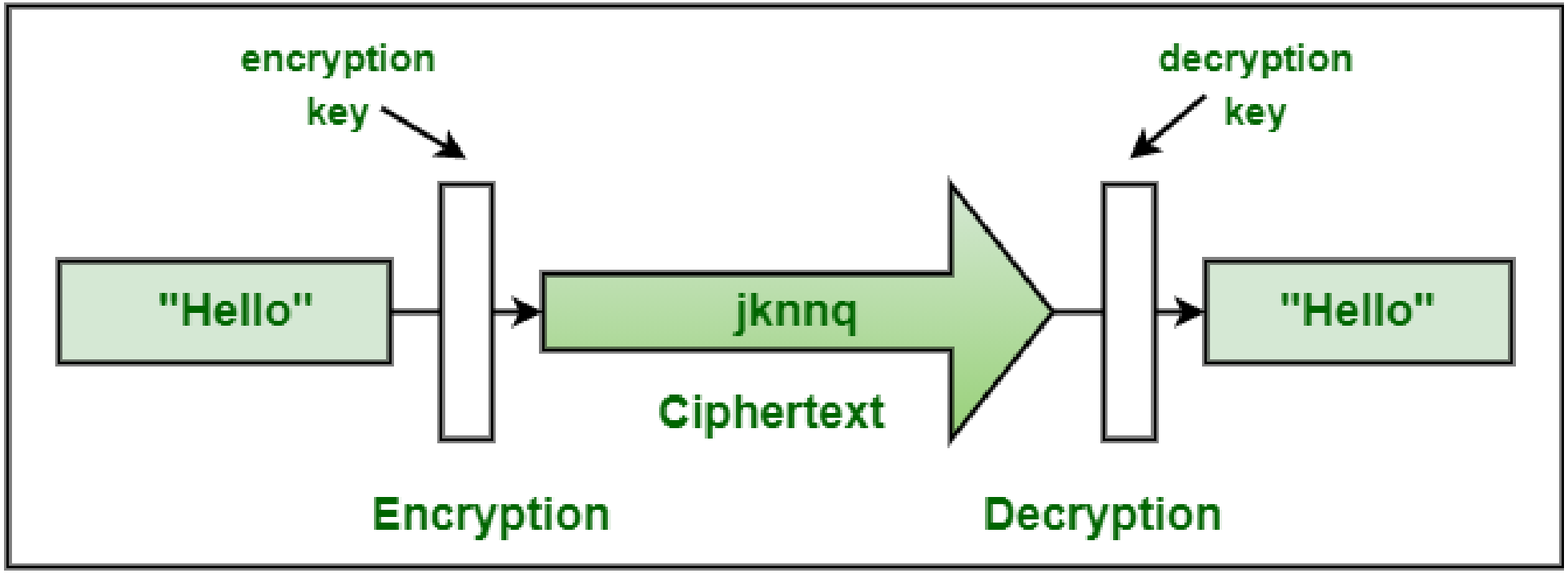
AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH USULLARI



KRIPTOGRAFIYA: ASOSIY TUSHUNCHALARI VA QISQACHA TARIXI



Kriptologiyaning *(kripto – yashirin, logiya – fan, bilim)* **rivojlanishini uchta bosqichga ajratish mumkin.**

Birinchi bosqich – kriptologiyani fan sifatidan e’tirof etilmagan davri, tor doiradagi qiziquvchilarga xos faoliyat turi bo‘lgan.

Ikkinchi bosqich 1949-yildan boshlanib, K.Shenonning «**Maxfiy tizimlarda aloqa nazariyasi**» nomli risolaning chop etilishi bilan bog‘lanadi. Bu risolada shifrlashning fundamental ilmiy tadqiqoti va uning mustahkamligi yoritib berilgan. Bu kitobning chop etilishi kriptologiya amaliy matematikaning tarkibiy qismi sifatida shakllanishiga asos bo‘ldi.

Uchinchi bosqich 1976-yilda U.Diffi va M.Xellman tomonidan «**Kriptografiyaning yangi yo‘nalishlari**» nomli asarning chop etilishi bilan belgilanadi. Unda maxfiy aloqa, yopiq kalitni avvaldan bermasdan ham, amalga oshirish mumkinligi bayon etilgan. Ushbu sanadan boshlab to hozirgi kungacha an’anaviy klassik kriptografiya bilan bir qatorda ochiq kalitli kriptografiyaning intensiv rivojlanishi davom etmoqda.

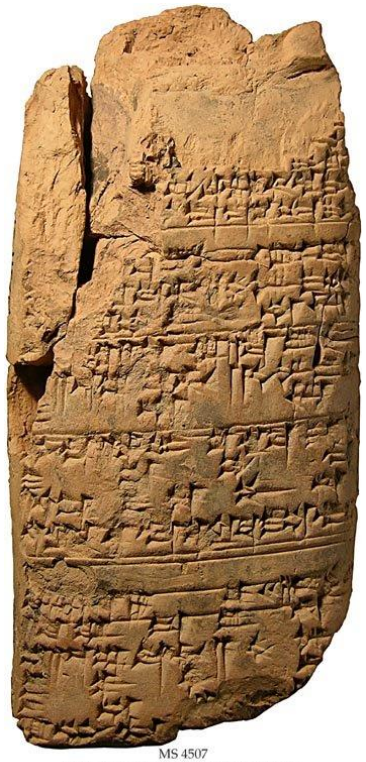
Kriptografiya axborotni muhofaza qilish usullaridan biri hisoblanadi. Kriptografiya axborot (ma’lumotlar)ni o‘zgartirish tamoyillari, vositalari va usullarini tadqiq etadi. Bundan maqsad axborot mazmunidan ruxsat etilmagan foydalanishdan muhofazalash va uni buzishni bartaraf qilish. Kriptografiya ma’lumotlarni aloqa kanallari orqali uzatishda yoki saqlashda konfedensiallikni yoki haqiqiylikni ta’minlash usullari bilan shug‘ullanadi. Shu bilan birga kriptografiya ma’lumotlarni xabardor bo‘lmagan shaxslar uchun tushuna olmaydigan qilish maqsadida o‘zgartirish usuli hamdir.

Ma’lumotlar xavfsizligi tizimining muhim tarkibiy bo‘lagi. Uning mohiyati ma’lumotlarni uzatishdan oldin **ma’nosiz belgilar** yoki **signallar yig‘masiga** aylantirish va ma’lumotlarni oluvchi qabul qilib olgandan so‘ng, ularni dastlabki shakliga qayta tiklashdir.

Insoniyat axborotni himoya qilish muammosi bilan yozuv paydo bo‘lgandan beri shug‘ullanadi. Bu muammo harbiy va diplomatik ma’lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartalilar harbiy ma’lumotlarni shifrlashgan. Xitoyliklar tomonidan oddiy yozuvni iyerogriflar ko‘rinishida tasvirlashlari uni xorijliklardan yashirish imkonini bergan.

«Kriptografiya» atamasi **grek** tilidan tarjima qilinganda «**yashirish, yozuvni berkitib qo‘ymoq**» ma’nosini bildiradi. Atamaning ma’nosi kriptografiya kerakli ma’lumotni yashirin saqlash va himoyalash maqsadida qo‘llanishini anglatadi. Kriptografiya axborotni himoyalash vositasi, shuning uchun u axborot xavfsizligini ta’minlashning bir tarmog‘i hisoblanadi.

Eramizdan oldingi XX asr. Mesopatamiyada o‘tkazilgan qazilmalar vaqtida eng qadimiy shifrlangan matnlar topilgan. Loydan yasalgan taxtachaga qoziqchalar bilan yozilgan matn hunarmandlarning sopol buyumlarini qoplash uchun tayyorlanadigan bo‘yoqning retsepti bo‘lib, u tijorat siri hisoblangan. Qadimgi misrliklarning diniy yozuvlari va tibbiyot retseptlari ham ma’lum.



MS 4507
Law codes of Eshnunna or Hammurabi.
Babylonia, ca. 1900-1650 BC

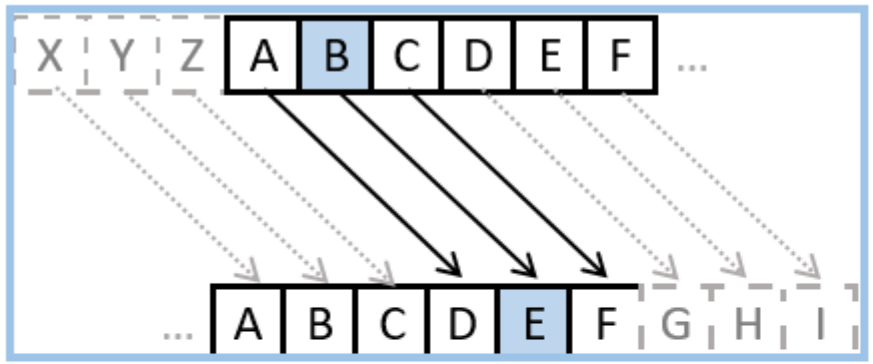
Eramizdan oldingi IX asrning o‘rtalari. **Plutarx** bergan ma’lumotlariga ko‘ra, ana shu davrda shifrlovchi qurilma – skital, qo‘llanilgan bo‘lib, u o‘rin almashtirishlar orqali matnni shifrlash imkonini bergan. Matnni shifrlashda so‘zlar biror diametrli silindrga (skitalga) o‘ralgan ensiz lentaga yozilgan. Lenta yoyilganda unda ochiq matn harflarining o‘rinlari almashtirilgan holati hosil bo‘lgan. Bunda kalit sifatida silindrning diametri xizmat qilgan. Bunday matnni shifrdan yechish usulini Aristotel taklif etgan. U lentani konusga o‘ragan va o‘qilishi mumkin bo‘lgan so‘z yoki so‘zning bir qismini ko‘rsatuvchi joy silindrning diametri deb hisoblagan.

Eramizning 56-yili. Y.Sezar gallar bilan urush vaqtida shirflashning almashtirish turini qo‘llagan. Ochiq matn alfaviti ostiga sikl bo‘yicha (Sezarda uchta pozitsiyaga) siljitish orqali shu alfavit yozilgan. Shifrlashda ochiq matndagi alfavitlar, ya’ni yuqori qismda joylashgan harflar quyi qismdagi mos harflar bilan almashtirilgan. Bu turdagi shifrlash Y.Sezargacha ma’lum bo‘lgan bo‘lsa-da, lekin bunday shifrlash usuli uning nomi bilan yuritiladi.

Kriptotahlil – bu kalitni bilmay turib, shuningdek, shifrlash algoritmi haqida ma’lumotlar yo‘q bo‘lgan holda yopiq axborotni shifrdan ochish jarayonidir.

Shifrning kriptomustahkamligi – samaradorlikning asosiy ko‘rsatkichi bo‘lib, u vaqt bilan yoki kriptotahlilchining kalit ma’lum bo‘lmagan holda shifrmatndan dastlabki ma’lumotni chiqarib olishi uchun kerak bo‘ladigan vositalar narxi bilan o‘lchanadi.

Keng qo‘llaniluvchi shifrlash algoritmlarini maxfiy saqlash mumkin emas. Shuning uchun shifrlash algoritmini yashirish zarurati yo‘q. U holda shifrlashning kriptomustahkamligi kalit uzunligi bilan belgilanadi. Chunki, yopiq axborotni shifrdan ochish uchun yo‘l faqatgina kalitni to‘g‘ri tanlashdir. Demak, kriptotahlilga ketadigan xarajat, ya’ni vaqt va mablag‘ kalitning uzunligi va shifrlash algoritmi murakkabligiga bog‘liq bo‘ladi.



SHIFT +3

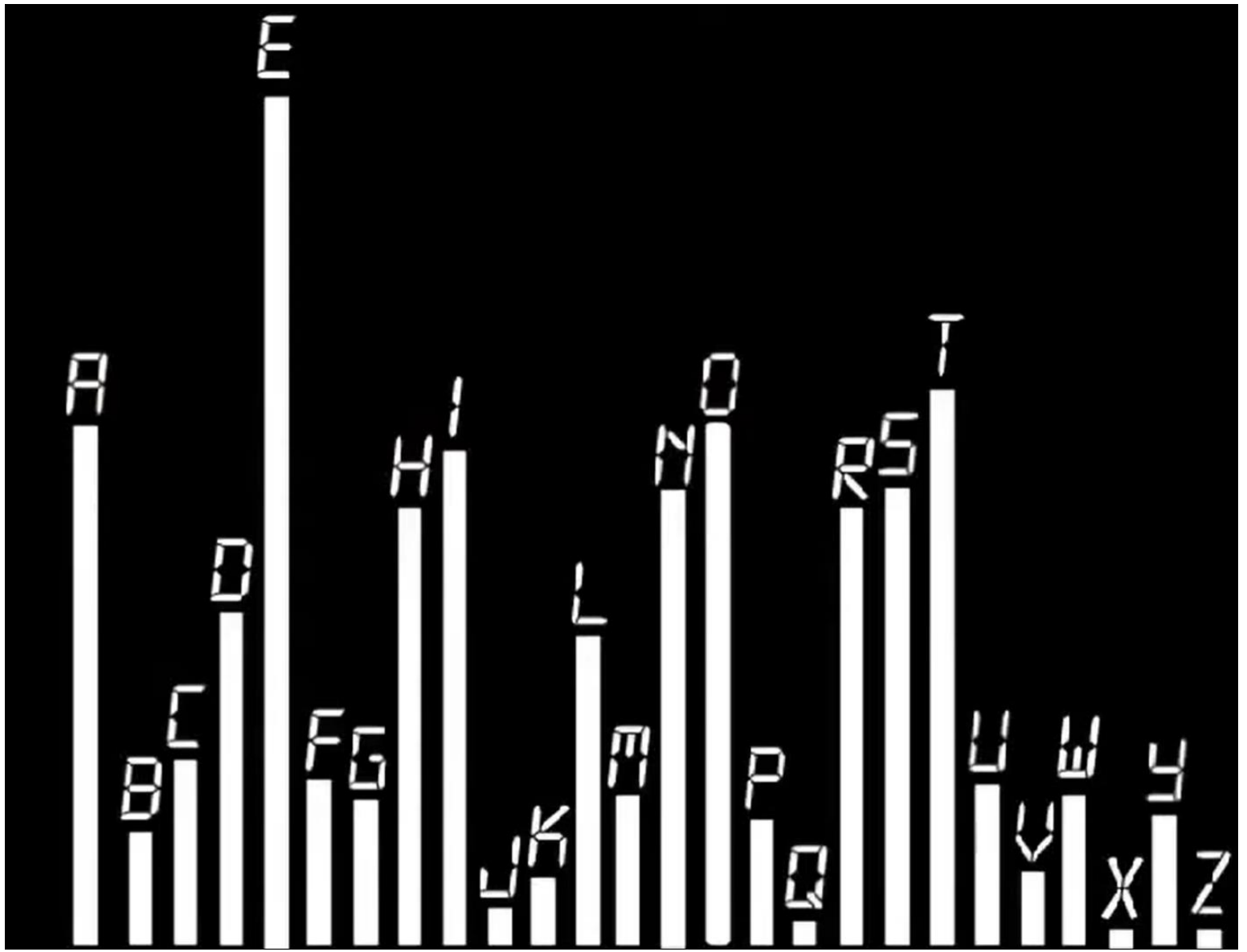
This Caesar cipher has a shift of 3 characters.

The letter ‘A’ becomes a ‘D’. The letter ‘B’ becomes ‘E’.

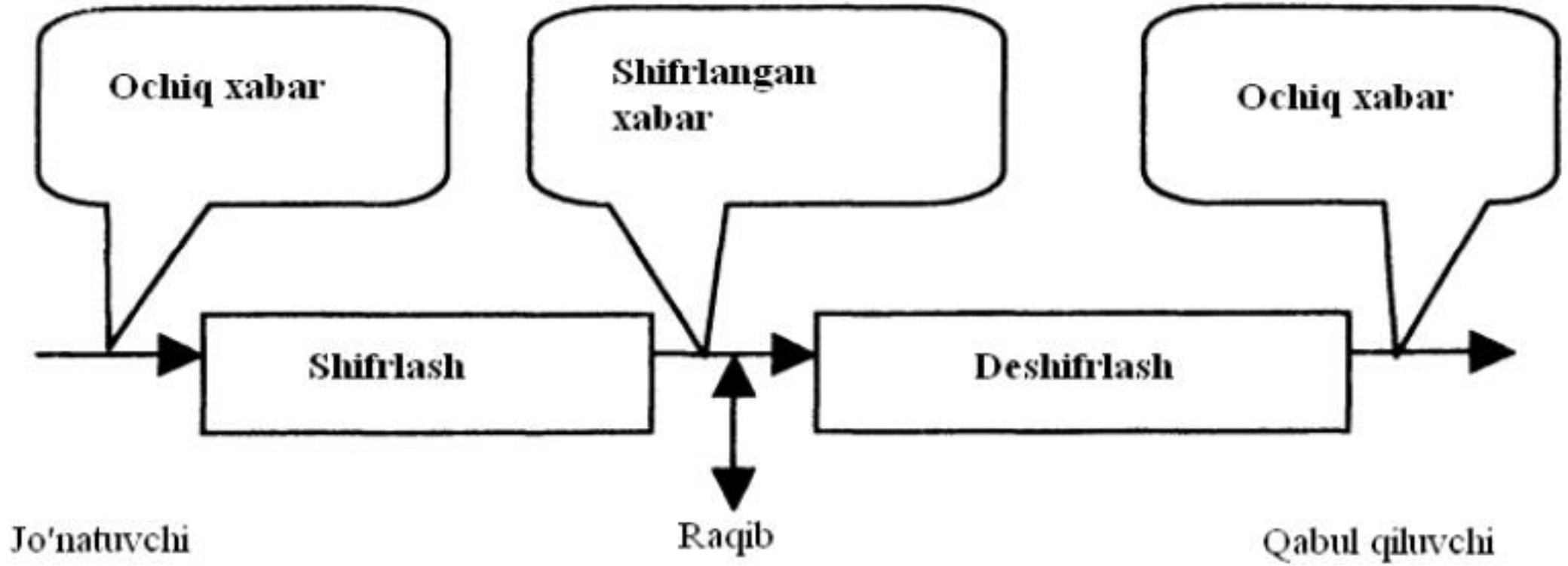
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plaintext

Ciphertext


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

Zamonaviy kriptografiya axborot xavfsizligining **konfedensiallik**, **butunlik**, **autentifikatsiya** va **tomonlarning mualliflikni inkor etolmasliklari** muammolarini hal etuvchi bilim sohasi hisoblanadi. Konfedensiallikni ta’minlash deganda axborot bilan tanishish huquqi bo‘lmagan shaxslardan bu axborotni himoyalash tushuniladi.



Raqib tomonidan nazoratda bo‘lgan aloqa kanali orqali uzatiladigan xabarning konfedensialligini ta’minlash muammosi kriptografiyaning an’anaviy masalalaridan hisoblanadi. Oddiy holda bu muammo uchta subyekt (tomonlar)ning o‘zaro munosabati sifatida bayon etiladi. **Axborot egasi** (jo‘natuvchi), raqibdan himoya qilish maqsadida, ochiq kanal orqali qabul qiluvchiga yuborilayotgan ochiq ma’lumotni o‘zgartiradi, ya’ni shifrlaydi.

Uzatilayotgan xabar ma’nosi bilan tanishish huquqi yo‘q subyekt raqibni anglatadi. Deshifrlash bilan shug‘ullanuvchi kriptotahlilchi ham raqib sifatida qaralishi mumkin. Olingan xabarni haqiqiy qabul qiluvchi deshifrlaydi. Raqib esa himoyalangan xabarga egalik qilmoqchi bo‘ladi, uning harakati hujum hisoblanadi. Hujum **faol** yoki **sust** bo‘lishi mumkin.

Sust hujum yashirin eshitish, trafikni tahlil qilish, shifrlangan xabarni qo‘lga kiritish, deshifrovka qilish, ya’ni himoyani «sindirish»ga qaratilgan harakatlar hisoblanadi. **Faol hujum**da raqib xabarni uzatish jarayonini to‘xtatib qo‘yishi, qalbaki xabarlar yuborishi yoki shifrlab uzatilayotgan xabarni modifikatsiya qilishi mumkin. Bu faol harakatlar mos ravishda imitatsiya qilishga va almashtirib qo‘yishga urinish hisoblanadi.

Kalit shifrlashning asosiy elementi bo‘lib, berilgan xabarni shifrlashdagi almashtirishlar u orqali amalga oshiriladi. Odatda, kalit harf va sonlarning biror-bir ketma-ketligidan iborat bo‘ladi. Har bir almashtirish kalit bilan bir qiymatli aniqlanadi va biror kriptografik algoritm orqali amalga oshiriladi. Shifrlashda bir kriptografik algoritm har xil rejimlarda qo‘llanishi mumkin. Shu tarzda har xil shifrlash usullari (oddiy almashtirish, gammalash va boshqalar) amalga oshiriladi. Har bir rejimning afzallik va kamchilik tomonlari mavjud. Shuning uchun rejimni tanlash konkret holatga bog‘liq. Deshifrlashdagi kriptografik algoritm, umumiy holda, shifrlashdagi algoritmdan farq qilishi mumkin. Bu holatda shifrlashdagi va deshifrovka qilishdagi kalitlar ham mos tushmasligi mumkin.

Shifrlovchi va deshifrovka qiluvchi algoritmlar juftligini **kriptotizim**, bu algoritmlarni amalga oshiruvchi qurilmani **shifrlovchi texnika** deyiladi.

Zamonaviy shifrlash usullari quyidagi talablarga javob berishi lozim:

A. shifrning mustahkamligi kriptotahlilga shunday qarshi tura olishi kerakki, bunda shifrdan ochish faqatgina kalitlarni to‘liq topish orqali amalga oshirilishi mumkin bo‘lsin;
B. kriptomustahkamlik shifrlash algoritmining maxfiyligi bilan emas, balki, kalitning maxfiyligi bilan ta’minlanishi lozim.
C. shifrmatn hajm jihatidan dastlabki axborotdan sezilarli darajada yuqori bo‘lib ketmasligi kerak;
D. shifrlash jarayonida yuzaga keladigan xatolar axborot buzilishi va yo‘qotilishiga olib kelmasligi kerak;
E. shifrlash vaqti katta bo‘lmasligi kerak;
F. shifrlash narxi shifrlanayotgan axborot qiymati bilan mos kelishi kerak.

Sodda shifrlar va ularning xossalari

An’anaviy (klassik) shifrlash usullariga o‘rinlarini almashtirish shifrlari, oddiy va murakkab almashtirish shifrlari va ularning kombinatsiyalari va modifikatsiyalari kiradi. Ta’kidlash joizki, o‘rinlarini almashtirish shifrlari va almashtirish shifrlarining kombinatsiyalari amaliyotda qo‘llanilayotgan har xil turdagi simmetrik shifrlarni tashkil etadi. O‘rinlarini almashtirish shifrlarida shifrlanadigan matnning harflari shu matn bloki ichida ma’lum qoidalar bo‘yicha o‘rin almashtiriladi. O‘rinlarini almashtirish shifrlari eng sodda va eng qadimiy hisoblanadi.

Shifrlovchi jadvallar. Tiklanish (XIV asr oxirlari) davrining boshlarida o‘rinlarini almashtirish shifrlarida shifrlovchi jadvallardan foydalanilgan. Shifrlovchi jadvallarning kaliti sifatida: jadvalning o‘lchami; o‘rin almashtirishni belgilovchi so‘z yoki jumla; jadval tuzilishining xususiyati bo‘lgan.

KALIT SIFATIDA JADVALNING O‘LCHAMI BERILISHI ENG SODDA JADVALLI SHIFRLASH HISOBLANADI.

Quyidagi matn berilgan bo‘lsin:

OBYEKT BELGILANGAN JOYGA BORADI

Ushbu axborot ustun bo‘yicha ketma – ket jadvalga kiritiladi:

O	K	L	A	N	G	R
B	T	G	N	J	A	A
Y	B	I	G	O	B	D
E	E	L	A	Y	O	I

Natijada, 4x7 o‘lchovli jadval tashkil qilinadi.

Endi shifrlangan matn qatorlar bo‘yicha aniqlanadi, ya’ni o‘zimiz uchun 4 tadan belgilarni ajratib yozamiz.

OKLA NGRB TGNJ AAYB IGOB DEEL AYOI

Bu yerda kalit sifatida jadval o‘lchovlari xizmat qiladi. Tabiiyki, uzatuvchi va qabul qiluvchi kalit jadval o‘lchami bo‘lishligini o‘zaro kelishib olishlari kerak. Deshifrlashda teskari amal bajariladi.

Kalit bo‘yicha oddiy o‘rnini almashtirish shifri

Bu usul oldingisiga nisbatan deshifrovka qilish uchun ancha murakkabdir. Bu usulda jadval ustunlari kalit bo‘luvchi so‘z, ibora, jumla orqali o‘rin almashtiriladi.

Misol tariqasida **UCHRASHUV INDINGA XIVA KINOTEATRIDA** matnini **TEGIRMON** so‘zini kalit sifatida qabul qilib, O‘rnini almashtirish shifrini qo‘llab shifrlaylik. Matnda 32 ta va kalitda 8 ta harflar borligi uchun 8x4 jadval tuzamiz.

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Endi kalit orqali 8x6 jadval tuzib kalitdagi harflarni alfavit bo‘yicha raqamlab chiqamiz.

T	e	g	i	r	m	o	n
8	2	1	3	7	4	6	5

U	A	V	I	X	K	T	R
C	S	I	N	I	I	E	I
H	H	N	G	V	N	A	D
R	U	D	A	A	O	T	A

Raqam bo‘yicha ustunlar o‘zgartiriladi.

g	e	i	m	n	o	r	T
1	2	3	4	5	6	7	8
V	A	I	K	R	T	X	U
I	S	N	I	I	E	I	C
N	H	G	N	D	A	V	H
D	U	A	O	A	T	A	R

Qator bo‘yicha 4 tadan bloklarga bo‘lib, simvollar ketma-ketligidagi shifrlangan matnni olamiz. Shuni e’tiborga olish kerakki, agar qatorda ketma-ket ikkita bir xil harf kelsa, chap tarafdan kelayotgan harf birinchi raqamlanadi, keyin esa ikkinchisi raqamlanadi va shifrlangan matn hosil qilinadi. Natijada quyidagi shifrlangan matn hosil bo‘ladi: VAIK RTXU ISNI IEIC NHGN DAVN DUAO ATAR Shifrni ochishda teskari jarayon amalga oshiriladi.

Shifrlangan matnning ochilishini yanada murakkablashtirish uchun u qaytadan shifrlanishi mumkin.

Bu usul **ikki tomonlama o‘rin almashtirish** shifri deyiladi. Bu usulda kalit sifatida ustun va qatordagi harflar tartibidagi sonlardan foydalaniladi. Avvalam bor kalit simvollariga qarab jadval tuziladi va ochiq matn joylashtirilib chiqiladi. so‘ngra raqamlar navbatma-navbat tartiblanib, avval ustun, keyin qatorlar o‘rni almashtiriladi va jadvaldagi ma’lumot qator bo‘yicha o‘qilib, shifrlangan matnga ega bo‘linadi.

Masalan: «**OBYEKT BUGUN KASAL**» ochiq matni shifrlash talab etilsin. Bu yerda kalit bo‘lib **1342** va **2341** xizmat qiladi. 4x4 jadval yaratib, ochiq matn qator bo‘yicha yoziladi

	2	3	4	1
1	O	B	Y	E
3	K	T	B	U
4	G	U	N	K
2	A	S	A	L

K_1

Endi qator va ustunlar tartib bo‘yicha o‘rinlari almashtiriladi.

	2	3	4	1
1	O	B	Y	E
2	A	S	A	L
3	K	T	B	U
4	G	U	N	K

	1	2	3	4
1	E	O	B	Y
2	L	A	S	A
3	U	K	T	B
4	K	G	U	N

Oxirgi jadvalga asosan shifrlangan matnni yozamiz va bloklarga bo‘lib chiqamiz.

EOBY LASA UKTB KGUN

Ikki tomonlama almashtirishda jadval kattaligiga qarab variantlar ham ortib boradi. Jadval o‘lchamining kattaligi shifr chidamliligini oshiradi: 3x3 jadvalda 36 ta variant, 4x4 jadvalda 576 ta variant, 5x5 jadvalda 14400 variant.

Mustaqil ta’lim savollari

1) **Kriptografiya va uning vazifasi?**
2) **Kriptotahlil va shifrning kriptomustahkamligi tushunchalariga ta’rif bering**
3) **Kriptologiyaning rivojlanish bosqichlari**
4) **Shifrlashni qadimgi tarixda qo’llanilishiga misollar keltiring**
5) **Sust hujum va faol hujum farqlari**
6) **Shiflashda kalit tushunchasi?**
7) **Zamonaviy shifrlash usullari qanday talablarga javob berishi kerak**
8) **Eng sodda jadvalli shifrlash usuli**
9) **Kalit bo‘yicha oddiy o‘rnini almashtirish usuli**
10) **Ikki tomonlama o‘rin almashtirish usuli**