13-Amaliy mashg'ulot.

Mavzu: Axborotlarni himoyalash usullari.

1.Ishdan maqsad: Simmetrik kriptotizimni asosiy usullarini o‘rganish va tadqiq etish.

2.Qisqacha nazariy ma’lumot:

Kriptografiya – axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.

Kalit – matnni shifrlash va shifrini ochish uchun kerakli axborot.

Kriptoanaliz – kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.

Kodlashtirish - esa axborotni ikkilik sanoq sistemasidagi “0” va “1” lardan iborat raqamli ko‘rinishidir.Agar axborotni shifrlash va uni qayta tiklash uchun bir xil kalitdan foydalanilsa bunday shifrlash usuli simmetrik shifrlash usuli deyiladi.

Kriptotizimlar simmetrik va ochiq kalitli tizimlarga bo‘linadi.

Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi.

***Ochiq kalitli kriptotizimlar*da** bir-biriga matematik usullar bilan bog‘langan *ochiq* va *yopiq* kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo‘ladi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi, yopiq kalit faqat qabul qiluvchigagina ma’lum.

Simmetrik shifrlash algoritmlarining turlari

Simmetrik shifrlash algoritmi to‘rtta turga bo‘linib , ular quyidagilar:

1. O‘rin almashtirish shifri.
2. Siljitish shifri.
3. Gammalashtirish shifri.
4. Shifrlash asosida shifrlashning analitik ifodasi.

O‘rin almashtirish shifri oddiy shifrlash hisoblanib, bu usulda qator va ustundan foydalaniladi. Chunki shifrlash jadval asosida amalga oshiriladi. Bu yerda kalit (K) sifatida jadvalning ustun va qatori xizmat qiladi. Matn (T0) simvollarining o‘lchamiga qarab NxM jadvali tuziladi va ochiq matnni (T0) ustun bo‘yicha joylashtirilib chiqiladi, qator bo‘yicha o‘qilib shifrlangan matnga (T1) ega bo‘linadi va bloklarga bo‘linadi.

Masalan, «Axborot xavfsizligi jadvali» matni shifrlansin.

T0=Axborot xavfsizligi jadvali;

K = 5x5; V=5;

A	O	F	I	D
X	T	S	G	V
B	X	I	I	A
O	A	Z	J	L
R	V	L	A	I

T1=AOFID_XTSGV_BXIIA_OAZJL_RVLAI

Birinchi bo‘lib, shifrlash jadvalidan (XIV asrning oxirlarida) diplomatik munosabatlarda, xarbiy sohalarda axborotni muhofazalashda foydalanilgan.

Oddiy o‘rin almashtirish usulidan tashqari kalit yordamida o‘rin almashtirish usuli ham mavjud. Shifrlash jadvalidan kalit orqali foydalaniladi.

Harf	Raqam	Harf	Raqam	Harf	Raqam	Harf	Raqam	Harf	Raqam
A	0	Z	8	P	16	CH	24	Q	32
B	1	I	9	R	17	SH	25	G‘	33
V	2	Y	10	S	18	‘	26	H	34
G	3	K	11	T	19	Ь	27	_	35
D	4	L	12	U	20	E	28		

YE	5	M	13	F	21	YU	29		
YO	6	N	14	X	22	YA	30		
J	7	O	15	S	23	O‘	31		

Bu yerda kalit simvollariga mos holda jadvalning o‘lchamiga qarab NxM jadvali tuziladi va ochiq matnni (T0) ustun bo‘yicha joylashtirilib chiqiladi. So‘ngra kalit simvollari alfavit tartibida tartiblanib, ustun bo‘yicha o‘rin almashtiriladi, qator bo‘yicha o‘qilib shifrlangan matnga (T1) ega bo‘linadi va bloklarga bo‘linadi.

T0= O‘zbekiston kelajagi buyuk davlat;

K = Toshkent;

V=4;

Matnda 28-ta va kalitda 7-ta harflar borligi uchun 7x7 jadval tuzamiz.

O‘	K	O	L	G	YU	V
Z	I	N	A	I	K	L
B	S	K	J	B	D	A
YE	T	YE	A	U	A	T

Endi kalit orqali 7x6 jadval tuzib kalitdagi harflarni alfavit bo‘yicha raqamlab chiqamiz.

T	o	sh	k	ye	n	t
5	4	7	2	1	3	6
O‘	K	O	L	G	YU	V
Z	I	N	A	I	K	L
B	S	K	J	B	D	A
YE	T	YE	A	U	A	T

Raqam bo‘yicha ustunlarni o‘zgartirib chiqamiz .

ye	k	n	o	T	t	sh
1	2	3	4	5	6	7
G	L	YU	K	O‘	V	O
I	A	K	I	Z	L	N
B	J	D	S	B	A	K
U	A	A	T	YE	T	YE

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.

T1= GLYUK UVOI AKIZ LNBJ DSBA KUUA TETE”;

Shifrni ochishda teskari jarayon amalga oshiriladi. Shifrlanish jarayoni qadamma – qadam amalga oshirilsa maqsadga muvofiq bo‘ladi.

Ikki tomonlama o‘rin almashtirish usuli. Bu usulda kalit sifatida ustun va qatordagi harflar tartibidagi sonlardan foydalaniladi. Avvalam bor kalit simvollariga qarab jadval tuziladi, va ochiq T0 matn joylashtirilib chiqiladi, so‘ngra esa raqamlar navbatma – navbat tartiblanib, avval ustun, so‘ngra esa qatorlar o‘rni almashtiriladi va jadvaldagi ma’lumot qator bo‘yicha o‘qilib T1ga ega bo‘linadi. Masalan: «Intilganga tole yor» ochiq matni shifrlash talab etilsin. Bu yerda kalit bo‘lib 1342 va 2314 xizmat qiladi. Yaxshiroq izohlanishi uchun K1=1342 va K2=2314, V=4 deb belgilab olamiz.

4x4 jadval yaratib T0 qator bo‘yicha yozamiz:

K_2

K_1	2	3	1	4
1	I	N	T	I
3	L	G	A	N
4	G	A	T	O
2	L	YE	YO	R

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

	2	3	4	1
1	I	N	T	I
2	L	YE	YO	R
3	L	G	A	N
4	G	A	T	O

	2	3	4	1
1	I	I	N	T
2	R	L	YE	YO
3	N	L	G	A
4	O	G	A	T

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

T1 =IINT_RLEYO_NLGA_OGAT

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;

Siljitish shifri. Siljitish shifri ikki turga bo‘linadi. Ular oddiy va murakkab siljitish shifrlaridir. Oddiy siljitish shifrida alfavit bo‘yicha siljigan harflar bilan shifrlanayotgan matn harflari alfavitga mos ravishda almashtirish orqali shifrlash amalga oshiriladi. Bir turli almashtirish shifri oddiy siljitish shifrining bir qismi hisoblanadi.

Sezarning shifrlash tizimi. Almashtirish usullari sifatida quyidagi usullarni keltirish mumkin: Sezar usuli, Affin tizimidagi Sezar usuli, tayanch so‘zli Sezar usuli va boshqalar.

Sezar shifri oddiy siljitish shifrining bir qismi hisoblanadi. Bu shifrni rimlik olim Gole Yuliy Sezar o‘ylab topgan. Shifrlashda matnning har bir harfi boshqa harf bilan quyidagi qoida asosida almashtiriladi. Harflarni almashtirishda kelayotgan yozuv harflarini K-ga siljitib almashtiriladi. Bu erda K–butun son hisoblanib uni quyidagicha ifodalash mumkin.

K=Kmod(m), m -alfavit soni . **Sezar usuli**da almashtiruvchi xarflar k va siljish bilan aniqlanadi. Yuliy Sezar bevosita k = 3 bo‘lganda ushbu usuldan foylangan.

k = 3 bo‘lganda va alifbodagi harflar m = 26 ta bo‘lganda quyidagi jalval hosil qilinadi:

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

Masalan, matn sifatida KOMPUTER so‘zini oladigan bo‘lsak, Sezar usuli natijasida quyidagi shifrlangan yozuv hosil bo‘ladi:

T1 = NRPSXWHU.

Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir.

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi: at+b (mod m), bu yerda a, b - butun sonlar, 0≤a, b<m.

m=26, a=3, b=5 bo‘lganda quyidagi jadval hosil qilinadi:

T	3t+5
0	5
1	8
2	11
3	14
4	17
5	20
6	23
7	26
8	29
9	32
10	35
11	38
12	41
13	44
1	47
15	50
16	53
17	56
18	59
19	62
20	65
21	68
2	71

Shunga mos ravishda harflar quyidagicha almashadi:

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

23	74
24	77
25	80
26	83

Y	T
Z	X

Natijada yuqorida keltirilgan matn quyidagicha shifrlanadi:
T1=PFXJDZSR

Kalit so‘zli Sezar tizimi. Sezarning kalit so‘zli shifrlash tizimi bitta alfavitli almashtirish tizimi hisoblanadi. Bu usulda kalit so‘zi orqali harflarning surishda va tartibini o‘zgartirishda foydalanadi. Lotin alifbosi asosida shifrlash. Kalit so‘zini tanlashda takrorlanmaydigan har xil harflardan iborat bo‘lgan so‘zni tanlash maqsadga muvofiqdir.Bu usul amalyotda qo‘llanilmaydi.Chunki kalit so‘zli Sezar shifrini kiriptotahlil asosida ochish mumkin.

3. Ishni bajarilish tartibi va qo‘yilgan vazifa:

Hisobot mazmuni:

1. Ish mavzusi.
2. Ishdan maqsad.
3. Shifrlash algoritmini blok-sxemasi.
4. Dastur matni.

Nazorat savollari

1. Kriptografiya maqsadi va vazifasi.
2. Oddiy o‘rin almashtirish usuli va kalit so‘zli o‘rin almashtirish usuli.
3. Ikki martalik qayta quyish usuli va sehrli kvadrat usuli.

Sezar usuli va kalit so‘zli Sezar tizimi