2.5. Sezar shifri

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

Sezar usulida almashtiriluvchi harflar k soniga siljishi bilan aniqlanadi. Yuliy Sezar bevosita k=3 bo‘lganda ushbu usuldan foydalangan.

k = 3 bo‘lganda va alfavitdagi harflar m = 26 ta bo‘lganda quyidagi jadval 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 KOMPYUTER so‘zini oladigan bo‘lsak, Sezar usuli natijasida quyidagi shifrlangan yozuv hosil bo‘ladi:

C = NRPSBXWHU.

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

Misol.

Bizga k-kalit, m-harflar soni, t-harflarning alfavitdagi tartib raqami, x-shifrlangan harf, M-shifrlanuvchi so‘z berilgan bo‘lsin.

(t+k) mod m = x →**shifrlash formulasi**;

(x-k) mod m = t →**shifrni ochish formulasi**;

Shifrlash:

M=”doska”;
K=3;
M=26;

d: (3+3) mod 26=6 →g
o: (14+3) mod 26=17 →r
s: (18+3) mod 26=21 →v
k: (10+3) mod 26=13 →n
a: (0+3) mod 26=3 →d

c=”grvnd”;

Shifrni ochish:
g: (6-3) mod 26=3 →d
r: (17-3) mod 26=14 →o
v: (21-3) mod 26=17 →s
n: (13-3) mod 26=10 →k
d: (3-3) mod 26=0 →a

M=”doska”

Nazorat uchun savollar:

1. Sezar usulida kalit nimadan iborat?
2. Kalit qaysi sondan qaysi songacha oraliqda bo‘ladi?
3. Shifrlanadigan matn harflari qaysi tartib bilan nomerlanadi?
4. Shifrlangan matnni ochishda modulda manfiy son chiqsa nima qilinadi?
5. Kalit har ikkala tomonda ham bo‘lishi shartmi?
6. Kalitsiz qanday ochish mumkin?

Mustaqil ish uchun misollar.

1. k=5, n=26: C=jsyjw, M=?
2. k=5, n=26: C=rtsnytw, M=?
3. k=5, n=26: C=xuehj, M=?
4. k=5, n=26: C=wzhmpe, M=?
5. k=5, n=26: C=vfqfr, M=?

6. k=6, n=26: C= ygrus, M=?
7. k=6, n=26: C= jkqgt, M=?
8. k=7, n=26: C= wypualy, M=?
9. k=7, n=26: C= uvrph, M=?
10. k=7, n=26: C= alslmvu, M=?
11. n=26: C=mjnad afxmds mjgvgyzuz smeaeukwadu zuetxmdu M=?
12. n=26: C=nkobebgk nisfvmyvt vfbknfvqntvk bmvetvkbyng M=?
13. n=26: C=olpcfchlojtgwnzwuwyohucfwmozofw M=?
14. n=26: C=pmqdgdiapgmxbdnphxpqhigpzibdsaapgx M=?
15. n=26: C= rkpyixdydwudwaefjqhgqbwqdkikbbqhy M=?
16. n=26: C=bizgkfcfxzprrjfjcrizrjfjzpkljyletyrcri M=?
17. n=26: C=sdygjalenscsdaldsjcjahlglarae M=?
18. n=26: C=lbffmk bdtezhkbmf etkhvabjdteb mebtezh kbmfetk M=?
19. n=26: C=elcjninurfcfufailcngrupzmctfcac M=?

2.6. Affin tizimi

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi: (a·t+b) mod m, bu yerda a, b - butun sonlar, 0≤a, b<m, a va m o‘zaro tub sonlar. t – harflarning alfavitda joylashgan tartibi (0 dan boshlab tartiblanadi), m – alfavitdagi harflar soni.

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

Shunga mos ravishda harflar quyidagicha almashadi:

A	F
B	J
C	N
D	R
E	S
F	V
G	Z
H	D
I	H

8	29
9	32
10	35
11	38
12	41
13	44
14	47
15	50
16	53
17	56
18	59
19	62
20	65
21	68
22	71
23	74
24	77
25	80
26	83

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
Y	T
Z	X

Natijada yuqorida keltirilgan matn quyidagicha shifrlanadi:
C=PFXJDZSR

Shifrni ochish formulasi quyidagicha: $M = \left(a^{-1}(C - b)\right) mod\ m.$ Bu yerda a^{-1} qiymat a sonining mod m bo‘yicha teskarisi, C – shifrtekst.

Nazorat uchun savollar:

1. Affin usulida kalit nimadan iborat?
2. Kalit qaysi sondan qaysi songacha oraliqda bo‘ladi?
3. Shifrlanadigan matn harflari nomerlanish tartibi qanday?
4. Shifrlangan matnni ochishda modulda manfiy son chiqsa nima qilinadi?
5. Kalit har ikkala tomonda ham bo‘lishi shartmi?
6. Kalitsiz qanday ochish mumkin?

Mustaqil ish uchun misollar.

1. a=5, b=11, n=26: C= zxuyzyptlnxlaz, M=?
2. a=5, b=12, n=26: C= jakdeqtmuumeczm, M=?
3. a=7, b=12, n=26: C= smimlmlmbnmzolq, M=?
4. a=9, b=11, n=26: C= frwrahgfthigfz, M=?
5. a=11, b=11, n=26: C= clcflulgabuly, M=?
6. a=17, b=11, n=26: C= rfayryjhluhnyr, M=?
7. a=19, b=11, n=26: C= mlerwlirwhzl, M=?
8. a=21, b=11, n=26: C= olonlctzxijxixzc, M=?
9. a=23, b=11, n=26: C= plrglgnheljq, M=?
10. a=3, b=11, n=26: C= zjyubznvtgjqjul, M=?
11. a=3, b=14, n=26: C= ehanoqmebtmlmygo, M=?
12. a=5, b=17, n=26: C= wjdatryfdaoreluf, M=?
13. a=7, b=19, n=26: C= otpwdistijtlxixpq, M=?
14. a=19, b=17, n=26: C= rlrssrcnenkrgrcnvu, M=?
15. a=25, b=11, n=26: C= slqtdnlhsdalid, M=?
16. a=23, b=12, n=26: C= swpcmrokwjwh, M=?
17. a=15, b=14, n=26: C= wijobwxwmwbnxoje, M=?
18. a=17, b=8, n=26: C= zyliamtgivwmlciteinil, M=?
19. a=19, b=17, n=26: C= krgrcnvuzrknsrc, M=?

2.7. Steganografiya

Steganografiya (grekcha στεγανοσ — yashirin va γραφω — yozayapman, sirli yozuv degan manoni anglatadi) — bu ochiq ma’lumotni uzatilayotgan vaqtda shifrni yoki sirni ichiga joylashtirib uzatishni o‘rganuvchi fan hisoblanadi.

Kriptografiyada shifr yoki sirli xabarning ko‘rinishi mavjud bo‘ladi, steganografiyada esa u ham sir saqlanadi. Steganografiyani, odatda,