MAVZU: AFFIN SEZAR SHIFRLASH ALGORITMI

Affin kriptotizimlari. Affin kripototizimlari keng tarqalmagan o‘rniga qo‘yish usullari sanalib, bir alfavitli shifrlash usullariga kiradi. Bu tizimlarga **affin tizimidagi Sezar usuli**, **ROT13** va **Atbash usullari** kiradi.

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi:

$$E(x)=ax+b\ (modm),$$

bu yerda a, b - butun sonlar bo‘lib, kalitlar hisoblanadi, 0≤a, b<m. *m* – alfavit uzunligi.

Deshifrlash jarayoni quyidagi formula asosida amalga oshiriladi:

$$D(E(x)) = a^{-1}(E(x) - b)modm.$$

Bu yerda a^{-1} *modm* bo‘yicha a ga teskari bo‘lgan son.

Lotin alfaviti foydalanilganda u quyidagicha raqamlanadi:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Shifrlash. Ushbu usulda ma’lumotlarni shifrlash uchun “**ATTACKATDAWN**” ochiq matni olinib, kalit sifatida a=3 va b=4 olindi. Alfavit uzunligi m=26 ga teng. Bu holda shifrlash funksiyasining umumiy ko‘rinishi quyidagicha bo‘ladi:$y = E(x) = (3x + 4)mod26.$ Yuqoridagi jadvalga asoslanib quyidagini olish mumkin:

Xabar	A	T	T	A	C	K	A	T	D	A	W	N
	0	19	19	0	2	10	0	19	3	0	22	13

Shifrlashning umumiy ko‘rinishi esa quyidagicha bo‘ladi:

Xabar	A	T	T	A	C	K	A	T	D	A	W	N
x	0	19	19	0	2	10	0	19	3	0	22	13
3x+4	4	61	61	4	10	34	4	61	13	4	70	43
(3x+4)mod26	4	9	9	4	10	8	4	9	13	4	18	17
Shifr matn	E	J	J	E	K	I	E	J	N	E	S	R

Deshifrlash jarayoni. Deshifrlash formulasi $D(y) = a^{-1}(y - b)modm$ ga teng bo‘lib, $a^{-1} = 9$, b=4 va m=26 ga teng bo‘ladi.

Shifr matn	E	J	J	E	K	I	E	J	N	E	S	R
	4	9	9	4	10	8	4	9	13	4	18	17

Deshifrlashning umumiy ko‘rinishi esa :

Shifrmatn	E	J	J	E	K	I	E	J	N	E	S	R
y	4	9	9	4	10	8	4	9	13	4	18	17
9(y-4)	0	45	45	0	54	36	0	45	81	0	126	117
9(y-4)mod26	0	19	19	0	2	10	0	19	3	0	22	13
Xabar	A	T	T	A	C	K	A	T	D	A	W	N

Olingan alfavitdagi barcha belgilarni shifrlash natijasi quyidagiga teng bo‘ladi.

Xabar	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
(3x+4)mod26	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1
Shifr matn	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B

A = 1	A' = 1
A = 3	A' = 9
A = 5	A' = 21
A = 7	A' = 15
A = 9	A' = 3
A = 11	A' = 19
A = 15	A' = 7
A = 17	A' = 23
A = 19	A' = 11
A = 21	A' = 5
A = 23	A' = 17
A = 25	A' = 25

Mustaqil ta’lim topshiriqlari.

1. Affin kripototizimlariga kiruvchi shifrlash usullarini keltiring.
2. Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar qaysi formula bo‘yicha aniqlanadi?
3. Affin tizimidagi Sezar usulida deshirlash qaysi formula bo‘yicha aniqlanadi?
4. Affin tizimidagi Sezar usulini bajarish ketma ketligini tushuntiring.
5. Atbash usuli haqida ma’lumot bering.