KRIPTOGRAFIYA TARIXI: QADIMGI SIVILIZATSIYALARDAN ZAMONAVIY ALGORITMLARGACHA

Ne'matova Hayitxon Nodirbek qizi
Farg'ona davlat universiteti
24-amaliy matematika yo'nalishi 1-bosqich magistranti
nematovahayitxon@gmail.com

Annotatsiya. Ushbu maqolada kriptografiyaning tarixi ko'rib chiqilgan. Ushbu maqolada yana Misr, Mesopotamiya, Sparta, Hindistondagi kriptografiya usullari haqidagi ma'lumotlar, Vizener shifrini qo'llash, Leon Albert diski haqida umumiy ma'lumotlar berilgan. Vizener shifrini C# dasturlash tilidagi dasturi.

Kalit so'zlar: Kriptografiya, shifrlash, deshifrlash, Mirs iyerogliflari, Mesopotamiya yozuvi, Sezar shifri, Skitali usuli, Vizener shifri, Leon Albert diski.

Kirish.

Kriptografiya insoniyatning maxfiylik va xavfsizlikka bo'lgan ehtiyojidan tug'ilgan. Qadimgi iyerogliflardan tortib, kvant shifrlashgacha bo'lgan yo'l inson aql-idroki va texnologiyaning ajoyib sintezidir. Kriptografiya bugun ham rivojlanib, ma'lumotlarni himoya qilishning yangi usullarini taklif etmoqda.

Kriptografiya - ma'lumotlarni shifrlash va shifrlash orqali ularni maxfiy saqlash va uzatishni ta'minlovchi fan va texnologiya hisoblanadi. Kriptografiya so'zi qadimgi yunoncha **"kryptos"** (maxfiy) va **"graphein"** (yozish) so'zlaridan olingan bo'lib, so'zma-so'z "maxfiy yozish" degan ma'noni anglatadi.

Kalit – kriptografiyada ma'lumotlarni shifrlash va deshifrlash jarayonlarida ishlatiladigan maxfiy ma'lumot hisoblanadi. Kalit kriptografik algoritmning asosiy qismi bo'lib, u shifrlash va deshifrlash jarayonlarini boshqaradi. Kalitning asosiy vazifasi ma'lumotlarning maxfiyligini ta'minlash hisoblanadi. Ya'ni faqat ruxsat etilgan shaxslar shifrlangan ma'lumotlarni o'qiy olishi yoki ma'lumotlarni tahrirlashi imkonini beradi. Zamonaviy kriptografiyada maxfiylik algoritm bilan emas, balki shifrlash kalitining maxfiyligi bilan ta'minlanadi, chunki algoritm oxir-oqibat qarshilik ko'rsatuvchi tomonidan aniqlanishi mumkin.

Shifr – bu ochiq matnlar to'plamini shifrlangan matnlar to'plamiga bir qiymatli akslantirishlar majmuasi bo'lib, u kalitlar to'plamidagi elementlar bilan indekslanadi: $\{Fk : X \to S, k \in K\}$.

Kriptografik tizim yoki **shifr** – bu ochiq matnlarni shifrlangan matnlarga aylantirish uchun ishlatiladigan matematik apparat va qoidalar majmuasi.

Shifrlash – bu ma'lumotlarni shifrlash yoki shifrdan ochish jarayonini anglatadi. Shuningdek, "shifrlash" atamasi ko'pincha "shifrlash" (ma'lumotlarni shifrlash) bilan

sinonim sifatida ishlatiladi. Biroq, "shifrlash" atamasini **"kodlash"** atamasi bilan almashtirish noto‘g‘ri, chunki kodlash odatda ma’lumotlarni belgilar (alifbo harflari) shaklida ifodalashni anglatadi.

Deshifrlash – bu kalit va, ehtimol, algoritm noma’lum bo‘lgan holda shifrlangan ma’lumotlarni ochiq ma’lumotlarga aylantirish jarayoni, ya’ni kriptoanaliz usullari yordamida amalga oshiriladi.

Kriptomustahkamlik – bu shifrning deshifrlashga qarshilik ko‘rsatish qobiliyatini belgilovchi xarakteristika bo‘lib, odatda deshifrlash uchun zarur bo‘lgan vaqt bilan o‘lchanadi.

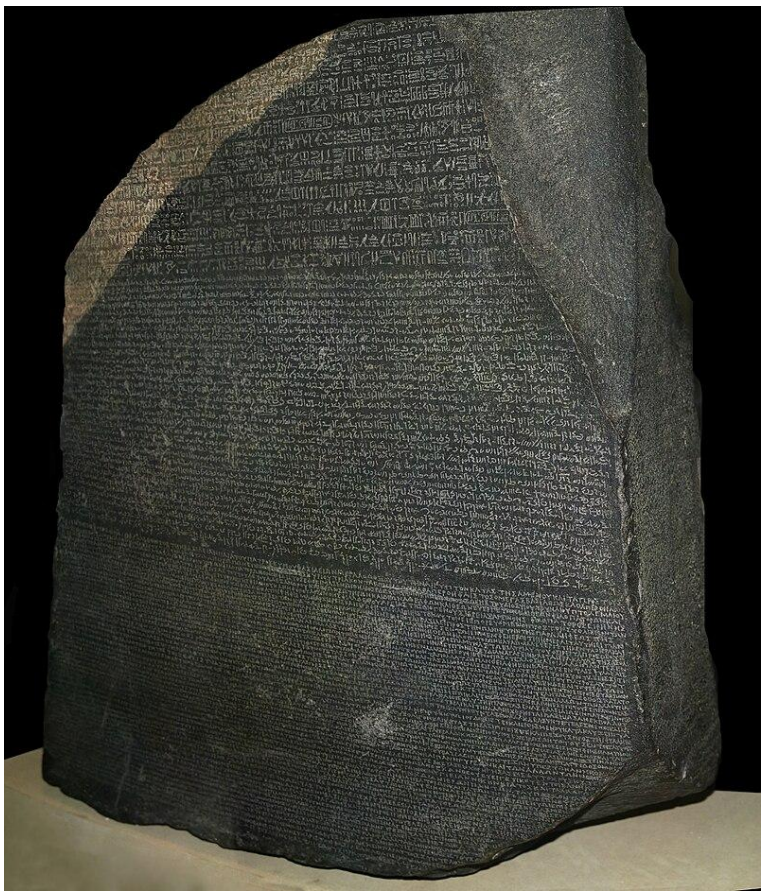
Ideogramma - bu narsa yoki fikrning nomini tashkil etuvchi tovushlarni ifodalamaydigan grafik rasm yoki belgi hisoblanadi. Ideogrammalardan foydalanish ideografiya deb ataladi.

Kriptografiyaning Qadimgi Davrlari

Qadimiy sivilizatsiyalar kriptografiya (shifrlash san’ati)ni rivojlantirishda muhim rol o‘ynagan. Misr, Mesopotamiya, Sparta, Rim Imperiyasi va Hindistonda bu usullar har xil maqsadlarda va turli texnikalar yordamida qo‘llanilgan.

Misr va Mesopotamiya - qadimgi sivilizatsiyalar bo‘lib, ularning yozuv tizimlari tarixda o‘ziga xos o‘’rniga ega. Misr va Mesopotamiya yozuv tizimlariga birinchi shifrlash usullari sifatida qaralishi mumkin, chunki ular yordamida ma’lumotlarni saqlash va uzatish uchun maxsus belgilardan foydalanilgan.

Misr iyerogliflari. Misrda iyerogliflar (qadimgi yunoncha ἱερογλύφος, hiéróglyphos; "hieros" – "muqaddas" va "glyphein" – "o‘ymoq") miloddan avvalgi 3000-yillardan boshlab ishlatilgan. Bu belgilarning bir necha turdagi shakllaridan iborat bo‘lib, ular tasviriy va fonetik tizimlarni o‘z ichiga olgan. Iyerogliflar asosan toshlarga, yodgorliklarga, piramidalar va boshqa yodgorliklarga o‘yib yozilgan. Misr yozuvi juda murakkab bo‘lib, uning to‘liq tushunilishi XIX asrda, Champollion(*Champollion le Jeune*) tomonidan Rosetta toshi yordami bilan amalga oshirildi. Bu topilma yordamida iyerogliflarning ba’zi qismlari deshifrlangan.



1-rasm. The Rosetta Stone in the British Museum.

Mesopotamiya Yozuvi. Mesopotamiya – qadimgi Sumer, Akkad, Babil va Assuriya kabi madaniyatlarning markazi hisoblanib, ular ham o‘zlarining yozuv tizimlari bilan mashhur. Mesopotamiya yozuvining eng mashhur turi bu kunli yozuv (cuneiform) bo‘lib, u miloddan avvalgi 3500-yillardan boshlab ishlatila boshlagan.

Kunli yozuv: Bu yozuv tizimi kumush yoki loyga bosilgan uzun pichoq kabi belgilarni o‘z ichiga olgan. Yozuvda pichoqning yassi uchlari yordamida tuzilgan belgilardan foydalanilgan. Kunli yozuv tasviriy belgilar bilan boshlanib, so‘ngra fonetik yozuvga o‘zgarib ketgan. Birinchi kunli yozuvlar asosan savdo, hisobotlar va ma’muriy ishlar bilan bog‘liq bo‘lgan. Kunli yozuv yordamida shaxsiy yozuvlar, hujjatlar, qonunlar va epik asarlar yozilgan. Eng mashhur asar bu "Gilgamesh" epikasidir, bu qadimgi Mesopotamiyadagi eng muhim adabiy asar hisoblanadi, uning parchalarini loy tabletalardan topishgan.

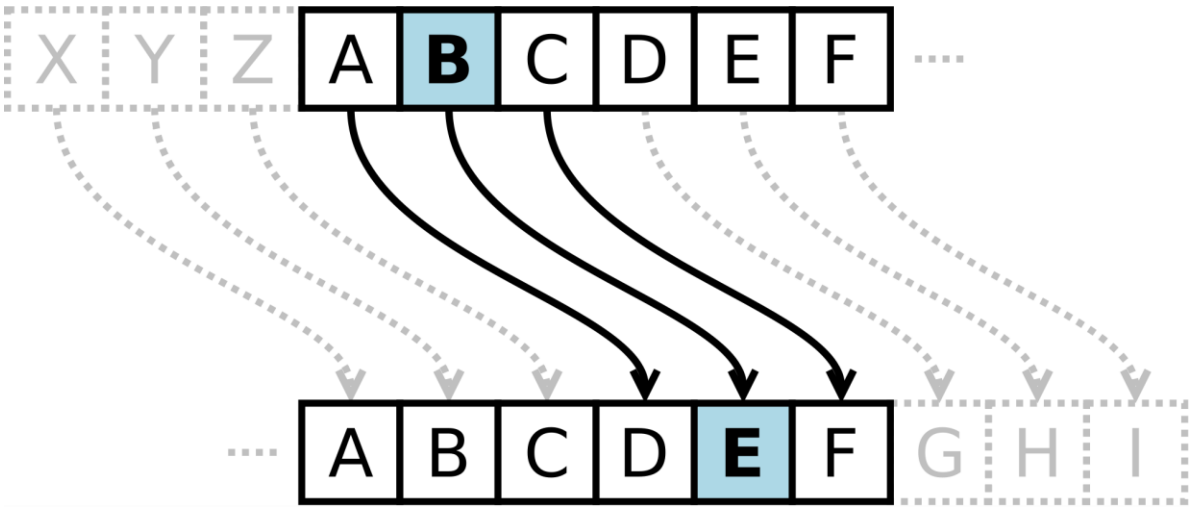
Misr va Mesopotamiya yozuv tizimlari birinchi shifrlash usullari sifatida qaralishi mumkin, chunki ular turli xil belgilarni ishlatgan va bu belgilar ma’lum bir xabarni yoki tushunchani ifodalagan. Bu tizimlar, ayniqsa, yozuvlarni dekodlash uchun maxsus bilimlarni talab qilgan. Misrda iyerogliflar ko‘proq diniy maqsadlar uchun, Mesopotamiyada esa iqtisodiy va siyosiy maqsadlar uchun ishlatilgan.

Skitala (Scytale) usuli. Sparta, qadimgi Yunonistonning eng mashhur va kuchli harbiy davlatlaridan biri bo‘lib, uning harbiy strategiyasi va sirli yozuv tizimlari juda muhim ahamiyatga ega bo‘lgan. Skitala (yunoncha "skytale" (σκυτάλη)— "palosli

tayoq") – bu Spartada harbiy maqsadlarda ishlatilgan birinchi shifrlash usuli hisoblanadi. Bu usulda xabar uzun va tor pergament (yoki charm) lentasiga yozilgan, so‘ngra maxsus diametrli yog‘och silindrga o‘ralgan. Faqatgina to‘g‘ri diametrli silindrga ega bo‘lgan qabul qiluvchi lentani silindrga o‘rab xabarni to‘g‘ri o‘qiy olgan. Agar dushman lenta qo‘lga kiritgan bo‘lsa, matn chalkash ko‘rinib, tushunarsiz bo‘lgan.. Bu usul juda sodda bo‘lib, lekin uni o‘qish uchun tayoqning o‘lchami va tartibi muhim bo’lgan. Shu sababli, agar tayoq yo‘qolsa yoki noto‘g‘ri o‘rab qo‘yilsa, xabarni tushunib bo‘lmasdi. Skitala usuli asosan harbiy maqsadlar uchun ishlatilgan, chunki bu xabarlarni raqiblardan yashirishda juda samarali bo‘lgan.

2-rasm. Skitala (Scytale) usuli

Sezar Shifri. Gay Yuliy Sezar (miloddan avvalgi 100–44) o‘zining harbiy xabarlarini shifrlash uchun Sezar shifri deb atalgan oddiy almashtirish usulidan foydalangan. Ushbu shifrning maqsadi harbiy va siyosiy xabarlarni maxfiy saqlash edi. Bu usul yog‘och yoki qog‘ozdagi harflarni boshqa harflarga ko‘chirish orqali amalga oshirilgan. Ushbu usulda har bir harf alifbo bo‘yicha ma’lum miqdorda siljigan (masalan, 5 ta harf keyinga surilgan). Shunday qilib, A → F, B → G va hokazo. Bu usulda, shifrlangan matnni faqatgina xabarni yuboruvchining va qabul qiluvchining biladigan ma’lum bir raqamli "kaliti" yordamida tushunish mumkin edi. Sezar shifri juda sodda va tez ishlovchi bo‘lib, asosan harbiy xabarlar va tizimlar uchun mo‘ljallangan edi. Ammo uning kamchiligi shundaki, uning oddiyligi sababli uni juda osonlik bilan yechib bo‘lar edi, shuning uchun u keyinchalik murakkabroq usullarga o‘zgartirildi. Sezar shifri tarixdagi eng mashhur va eng qadimgi shifrlash usullaridan biri hisoblanadi. Misol tariqasida "ATTACK" so’zini olsak, shifrlangandan so’ng matn ushbu matnga o’tadi: "DWWDFN"



3-rasm. Sezar shifri

Hindiston: Kautilya tomonidan tavsiflangan kriptografik usullar. Hindiston tarixidagi eng mashhur siyosatchi va faylasuflardan biri bo‘lgan Kautilya (yoki Chanakya) o‘zining "Arthashastra" asarida bir nechta kriptografik usullarni tavsiflagan. Arthashastra - bu qadimgi Hindistonning siyosiy, iqtisodiy va harbiy bilimlar to‘plami bo‘lib, unda kriptografiya bilan bog‘liq bir nechta muhim tamoyillar mavjud. Kautilya o‘z asarida bir nechta shifrlash usullarini, jumladan mahfiy yozuvlar va symbolik yozuvlarni tasvirlagan.

Kautilya tomonidan tavsiflangan ba’zi kriptografik usullar:

- ✓ **Shifrlangan yozuvlar**: Kautilya "Arthashastra"da shifrlangan yozuvlarni ishlatishning ahamiyatini ta’kidlagan. U, masalan, xabarlarni yozishda harflarni almashtirish yoki maxfiy so‘zlar bilan yozish kabi usullarni ishlatishni tavsiya etgan.
- ✓ **Jismoniy va maxfiy belgilardan foydalanish:** Kautilya xabarlarni yuborishda maxfiy belgilardan foydalanishni ham nazarda tutgan. Bunday belgilarning ma’nosi faqat ma’lum odamlar uchun tushunarli bo‘lishi kerak edi.
- ✓ **Kodlangan xatlar va maxfiy ismlar**: Xatlar va xabarlar uchun maxfiy kodlar ishlatish, masalan, shaxslar yoki joylar nomlarini kodlash kabi usullarni tavsiya qilgan.

Vizener shifri (frantsuzcha: visener shifri) Chiffre de Vigenère) - kalit so‘z yordamida harf matnini polialfavit shifrlash usuli hisoblanadi. Garchi Alberti, Trithemius va Porta vizener shifrini yaratishda katta hissa qo‘shgan bo‘lsalarda, shifrning yakuniy shaklini bergan odam sharafiga ya’ni Blaise de Vigenère sharafiga vizener shifrlash deb nomlanadi. vizener shifrining kuchliligi shundaki, u xabarni shifrlash uchun bir emas, balki 26 xil shifr alifbosidan foydalanadi. Shifrlash quyidagi jadvalda ko‘rsatilgan vizener kvadratini qurishdan boshlanadi: ochiq matn alifbosi, undan keyin har biri oldingi alifboga nisbatan bitta harfga siljigan 26 ta shifrlangan alifbo.

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

4-rasm. Vizener shifri

Ushbu jadval asosida vizener shifrlash amalga oshiriladi. Ushbu usulda ustunda asosiy matn harflari joylashga. Satrda esa kalitning harflari joylashgan bo'ladi. vizener shifrlashda ilk ishimiz kalit so'zini tanlashdan iborat bo'ladi. So'ngra esa shifrlamoqchi bo'lgan matnimizning uzunligiga mos qilib kalitni yozib olamiz. Keyingi qadamimiz esa ustundan shifrlanayotgan matndagi harf tanlanadi. Keyin esa shu harfga mos kalit harfi tanlanadi. Ular kesishgan joydagi harf yoziladi. Bu ketma - ketliki har bir harf uchun yozib chiqaldi. So'ngra vizener shifrida shifrlangan matnga ega bo'lamiz. Misol tariqasida "Ishon, harakat qil, yetish"ushbu matnni vizener shifrida shifrlab ko'ramiz:

Asosiy matn:Ishon, harakat qil, yetish

Kalit so'z: sabr

Endi shifrlashni boshlaymiz: Avval kalit so'znini va Asosiy matnni probel, tinish belgilarsiz yozib olamiz.

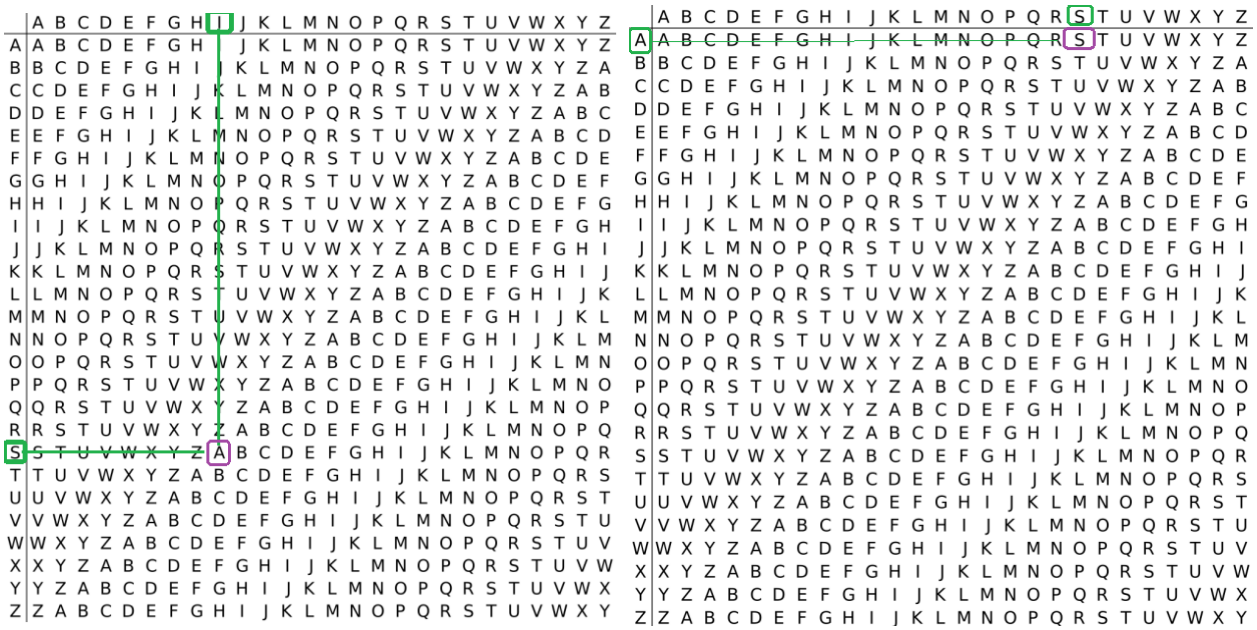
Asosiy matn: Ishonharakatqilyetish

Kalit so'z: sabr

Keyingi qadam esa kalit so'zini asosiy matndagi belgilar soniha yozib olishdan iborat bo'ladi. Asosiy matnimiz 21 ta belgidan iborat. Kalit so'zini 21 belgidan iborat qilib olamiz. Bularni tushunarli bo'lishi uchun jadvalda ko'rsataman:

Kalit so'zi	s	a	b	r	s	a	b	r	s	a	b	r	s	a	b	r	s	a	b	r	s
Asosiy matn	i	s	h	o	n	h	a	r	a	k	a	t	q	i	l	y	e	t	i	s	h
Shifrlangan matn																					

Keyin aytib o’tkanimdek, vizener kvadratidan foydalanamiz.



Ushbu amallarni har bir had uchun bajarib chiqamiz. Va yuqoridagi jadvalni to’ldirib chiqamiz:

Kalit so’zi	s	a	b	r	s	a	b	r	s	a	b	r	s	a	b	r	s	a	b	r	s
Asosiy matn	i	s	h	o	n	h	a	r	a	k	a	t	q	i	l	y	e	t	i	s	h
Shifrlangan matn	A	S	I	F	F	H	B	I	S	K	B	K	I	I	M	P	W	T	J	J	Z

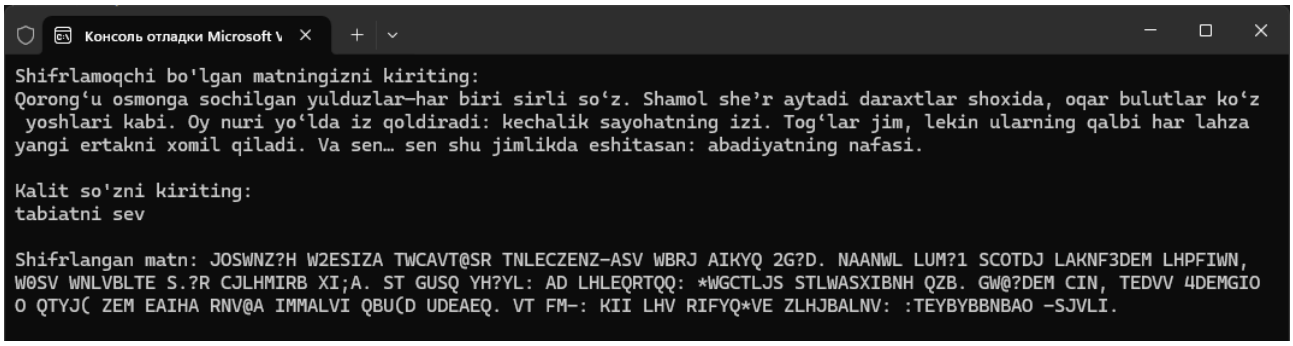
Amallarni bajarib bo’lganimizdan so’ng bizda shifrlangan matnga ega bo’lamiz. Bizning shifrlangan matnimiz quyidagicha bo’ldi: asiff, hbiskbk iim, pwtjjz

Leon Alberti disk. Eng birinchi kriptografik qurilma 15-asrda italyan arxitektori va ko‘p alifboshifrining otalaridan biri hisoblangan **Leon Battista Alberti** tomonidan ixtiro qilingan **shifrlash diski** bo’lgan. U ikki mis diskni (biri boshqasidan biroz kengroq) olib, ikkala diskning chetiga alifbo harflarini joylashtirga. Kichikroq diskni kattasining ustiga qo‘yib, ularni mil (o‘q vazifasini bajaruvchi) bilan birlashtirib, rasmda ko‘rsatilgan shifrlash diskini yaratdi. Bu disklar mustaqil ravishda aylantirilishi mumkin bo’lgan, shu bilan birga ikkala alifbo bir-biriga nisbatan turli holatlarni egallab, oddiy Sezar shifri orqali xabarlarni shifrlash uchun ishlatilardi. Sezar shifri bilan **1 pog‘ona siljish** uchun tashqi diskdagi **A** harfini ichki diskdagi **B** harfiga qarata sozlang. Tashqi disk oddiy matn (ochiq matn) alifbosi, ichki disk esa shifrlash alifbosi bo‘ladi. Xabardagi ochiq matn harfi tashqi diskda topiladi va unga mos keladigan ichki diskdagi harf shifrmatn qismi sifatida yoziladi. **5 pog‘ona siljish** bilan shifrlash uchun disklarni shunday aylantiringki, tashqi diskdagi **A** harfi ichki diskdagi **F** harfiga to‘g‘ri kelsin. **Leon Battista Alberti** risolasida o‘zining shifrini o‘z ichiga olgan bo‘lib, u "shohlarga loyiq shifr" deb atagan. Uning ta’kidlashicha, bu shifrni ochib bo‘lmaydi. Shifrni amalga oshirish shifrlash diskidan foydalangan holda amalga oshirildi, bu

polialfavit almashtirishlarning butun seriyasining boshlanishini belgiladi. Shuni ham ta’kidlash joizki, Yevropadagi kriptoanalizga bag‘ishlangan birinchi kitoblardan biri “Shifrlar haqida risola” (1466) italiyalik olim, gumanist, yozuvchi, yangi Yevropa me’morchiligi asoschilaridan biri Leon Battista Alberti tomonidan yozilgan va Uyg‘onish davri san’atining yetakchi nazariyotchisi. Uning faoliyati kriptografiya rivojiga katta hissa qo‘shdi inson bo’lgan.

5-rasm. Leon Alberti disk.

Endi vizener shifrini C# dasturlash tilidagi dasturini tuzamiz. Buning uchun Console oynasidan foydalanamiz. Va ikkita metoddan foydalanamiz. Birinchisi Matnni shifrlash uchun ishlatilsa, ikkinchi shifrlangan matnni deshifrlash uchun ishlatildi. Quyida tayyorlangan dastur yordamida matnni shifrlangan so’ng paydo bo’lgan matn berilgan.



Foydalanilgan adabiyotlar:

1. **"The Hieroglyphs of Ancient Egypt"** - Lesley and Roy Adkins.
2. **"Mesopotamia: The Invention of the City"** - Gwendolyn Leick.
3. **"A History of Writing"** - Steven Roger Fischer.
4. "The Code Book" by Simon Singh
5. "The Codebreakers" - David Kahn

6. "Greek and Roman Technology" K.D. White
7. "De Vita Caesarum" (Sezarlar hayoti) - Suetonius
8. "Cryptography and Network Security" - William Stallings
9. "Arthashastra" - Kautilya
10. "Cryptology in Ancient and Medieval India"