

59–60-darslar. MA'LUMOTLARNI SHIFRLASH. SHIFRLASH USULLARI

1. Shifrlash nima va u nima uchun kerak?

2. Ma'lumotlar qanday shifrlanadi?

Axborotni ruxsat etilmagan foydalanuvchidan yashirish, ma'lumot ma'nosini tushunib olmaslik uchun uni tushunarsiz holatga o'tkazish kriptografik (maxfiy belgilar bilan yozish) himoya usullaridan biri sanalgan shifrlash usullari asosida amalga oshiriladi. Shifrlash usullari yordamida ochiq ma'lumot yashiringan ko'rinishdagi shifrmtn holatiga aylanadi. Bu esa undan buzg'unchi tomonidan foydalanishning oldini oladi.

Ma'lumot maxfiyligiga shifrlash orqali erishiladi. Kriptografiya nuqtayi nazaridan olganda, shifr bu kalit bo'lib, u ochiq ma'lumotlar to'plamini yopiq (shifrlangan) ma'lumotlarga o'zgartirish uchun ishlatiladi.

Texnik nuqtayi nazardan olganda esa shifrlash odamlar o'qiy oladigan oddiy matnni tushunarsiz matn, ya'ni shifrlangan matnga aylantirish jarayoni hisoblanadi. Sodda aytganda, shifrlash dastlabki matnni oladi va undagi simvollarni tasodifiy ko'rinadigan qilib o'zgartiradi.

Shifrlash ikki xil bo'lishi mumkin: simmetrik shifrlash va assimetrik shifrlash.

Simmetrik shifrlash ma'lumotlar xavfsizligini ta'minlashning oddiy va an'anaviy usuli hisoblanadi. Simmetrik shifrlash shifrlash va deshifrlashni bitta kalit orqali amalga oshiruvchi algoritmlarni o'z ichiga oladi.

Simmetrik shifrlash usuli quyidagi vizual ko'rinishga ega:



TAYANCH TUSHUNCHALAR

Matn – alifbo belgilarining tartiblangan ketma-ketligi.

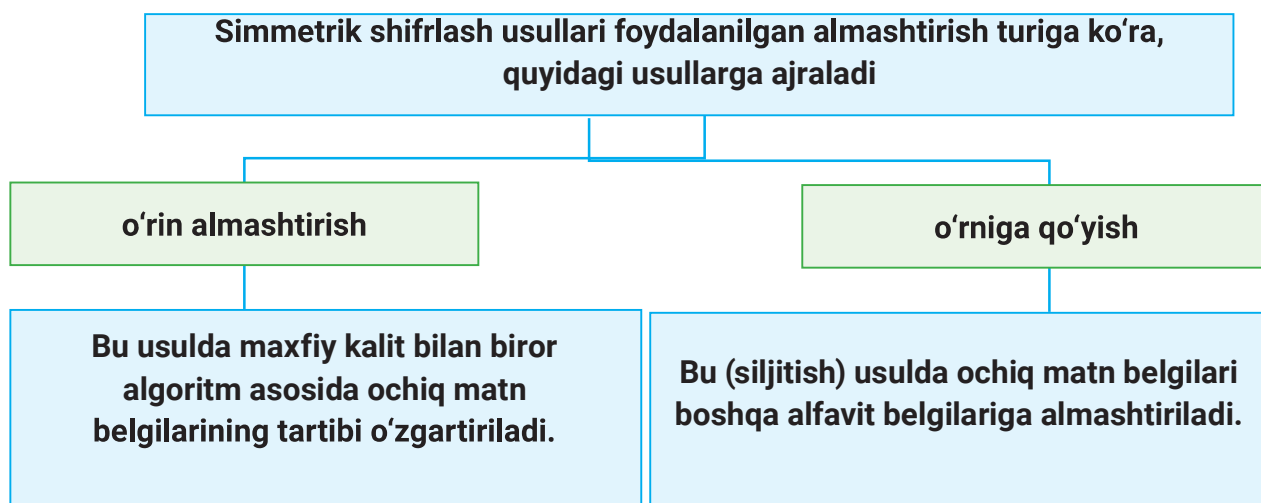
Shifrlash – ochiq (dastlabki) matnni kalit yordamida shifrlangan matn holatiga o'tkazish.

Deshifrlash – shifrlashga teskari jarayon. Bunda kalit yordamida shifrlangan matn dastlabki matn holatiga o'tkaziladi.

Shifr (kalit) – dastlabki matnni shifrlash va deshifrlash uchun zarur ma'lumot.

Axborotni shifrlash – ochiq axborot (dastlabki matn)ni shifrlangan axborotga o'zgartirish va aksincha, shifrlangan axborotni dastlabki matn ko'rinishiga qaytarish jarayoni.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA



O'rin almashtirish usuli

Shifrlashning o'rin almashtirish usuli oddiy shifrlash hisoblanib, bunda berilgan matnda ishtirok etgan belgilar o'rnini maxsus qoida asosida almashtiriladi. O'rin almashtirishga misol tariqasida, dastlabki axborot blokini jadvalga ustun bo'yicha yozishni, o'qishni esa satr (qator) bo'yicha amalga oshirishni ko'rsatish mumkin. Jadval qatorlarini to'ldirish va shifrlangan axborotni ustun bo'yicha o'qish ketma-ketligi kalit yordamida berilishi mumkin. Bunda jadvalning ustun va qatorlari kalit (K) sifatida xizmat qiladi.

O'rin almashtirish usuli yordamida shifrlash ketma-keligi:

- 1) matn(T_0)dagi simvollar soniga qarab, $N \times M$ o'lchamli jadval tuziladi. Bu yerda jadval o'lchamlari kalit sifatida xizmat qiladi;
- 2) dastlabki, ya'ni ochiq matn (T_0) ustun bo'yicha yozib chiqiladi;
- 3) keyin jadvaldagi ma'lumot qator bo'ylab yoziladi. Shifrlangan matn (T_1) ustun bo'ylab o'qiladi;
- 4) shifrlangan matn bloklarga ajratiladi, ya'ni satrlar soni qancha bo'lsa, belgilar shunchadan ajratib yoziladi.

Endi o'rniga qo'yish usuliga doir misolni ko'rib chiqamiz.

1-mashq. "Dushmanga nafrati bo'lmaganing Vatanga muhabbati bo'lmas" matnini o'rin almashtirish usulida shifrlang.

Yechim:

T_0 = "Dushmanga nafrati bo'lmaganing Vatanga muhabbati bo'lmas" matnida 49 ta simvol ishtirok etgan. $N = 7$, $M = 7$, $K = 7 \times 7$. 7 ta ustun va 7 ta satrdan iborat jadval tuziladi.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

1) Shifrlanishi kerak bo'lgan ochiq matn (to) ustun bo'yicha yozib chiqiladi;

2) jadvaldagi ma'lumotni ustun bo'ylab yozib, T_1 shifrlangan matn hosil qilinadi:

$T_1 = \text{DAIAAUIUNBNTHBSHAO'NAAO'MFLINBL}$

$\text{ARMNGBMNAAGAAAGTGVM TS.}$

Satrlar sonidan $V = 7$ ekanligi aniqlanadi va shifrlangan matn quyidagi ko'rinishda bloklarga ajratiladi:

$T_1 = \text{DAIAAUI_UNBNTHB_SHAO'NAAO'_MFLINBL_}$
 $\text{ARMNGBM_NAAGAAA_GTGVM TS.}$

D	A	I	A	A	U	I
U	N	B	N	T	H	B
SH	A	O'	N	A	A	O'
M	F	L	I	N	B	L
A	R	M	N	G	B	M
N	A	A	G	A	A	A
G	T	G	V	M	T	S

Bu usulda uzatuvchi va qabul qiluvchi foydalanuvchilar kalit jadval o'lchami bo'lishligini o'zaro kelishib olishlari lozim. Asl matnni hosil qilishda, ya'ni deshifrlashda yuqoridagi amallarga teskari amal (T_1 matn jadvalga satr bo'ylab yozish va ustun bo'ylab o'qish) bajariladi.

O'rniga qo'yish usuli

Bu usulda almashtirilishi kerak bo'lgan belgi alifboda o'zidan K ta keyin joylashgan belgi bilan o'zgartiriladi. Simmetrik shifrlash jarayoniga oid yana bir misolni ko'ramiz:

Toshkent shahrida Javohir va Nuriddin ismli ikki do'st yashaydi. Ayrim sabablarga ko'ra, Javohir shaharni tark etishi lozim. Ular o'zaro bog'lanishining yagona yo'li – pochta aloqasi. Ammo ular kimdir maktubni o'qishi mumkinligidan qo'rqadi. Muammoni qanday hal qilish mumkin?

Yechim. Javob esa oddiy. Maktubni kimningdir ko'zidan himoya qilish uchun ular o'z xabarlarini quyidagicha yozishga qaror qilishadi: xabarning har bir harfi alifbo bo'yicha o'zidan keyin kelgan 7-harf bilan almashtiriladi. Shunday qilib, ular **"SALOM"** so'zining o'rniga **"O'ISVT"** (SO', AI, LS, OV, MT) deb yozadi.

Xat mazmuni

"Salom Nuriddin, men onlayn biznes bilan shug'ullanishni boshladim. To'lovlarning aksariyati mening veb-saytim orqali olinadi. Men o'z mijozlarim ma'lumotlarini himoya qilish uchun eng yaxshi shifrlash usuliga ega bo'lishni xohlayman. Nuriddin, menga qanday maslahat bera olasiz? Hurmat bilan Javohir."

Ma'lumotni asl holiga qaytarish uchun esa ular xabarning har bir harfini alifbo bo'yicha o'zidan oldin kelgan 7-harf bilan almashtirishadi.

Bu **Sezar shifri** deb ataluvchi oddiy shifrlash usuli edi. Odatda, bu usulda dastlabki matnning har bir harfi alifboda o'zidan keyingi 3-harf bilan almashtiriladi. Umumiy holatda esa siljish turlicha bo'lishi mumkin, bu alifbodagi harflar soniga bo'g'liq.

Bu usul juda oddiy usul sanaladi. Bugungi shifrlash usullari u qadar sodda emas.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

Keng qo'llaniladigan shifrlash algoritmlari shu qadar murakkabki, hatto ko'plab super kompyuterlarning birlashtirilgan hisoblash kuchi ham ularni "sindira" olmaydi.

Assimmetrik shifrlashda shaxsiy kalitlardan foydalaniladi. Bu usul 2 ta: bitta ochiq va bitta yopiq kalit bilan ishlaydi. Ochiq kalitni hammaga berish mumkin, ammo yopiq kalit albatta maxfiy qolishi lozim. Chunki ma'lumot yoki xabarlar ochiq kalit yordamida shifrlansa, yopiq kalit yordamida deshifrlanadi.

Deylik, maxfiy ma'lumotlar saqlangan qutiga 2 ta kalit qo'yilgan. Ulardan faqat bittasi asosiy kalit hisoblanadi va unga hamma ega bo'lishi mumkin.

Ikkinchi kalit esa sizga va qutini yuborayotgan do'stingizga ma'lum qilinishi mumkin. Siz qutini do'stingizga boshqa shaxs orqali berib yuborasiz. U ochishga urinib ko'radi, chunki unda qulfni ochish uchun bitta kalit bor. Afsuski, uning urinishi muvaffaqiyatsiz tugallanadi va do'stingizga qutini butunligicha yetkazib beradi. Do'stingiz esa ikkinchi kalit yordamida qutidagi shifrlangan ma'lumotlarni bema'lol o'qiy oladi.

Assimmetrik shifrlash usuli quyidagi vizual ko'rinishga ega:

Aa	Bb	Dd	Ee	Ff	Gg
Hh	Ii	Jj	Kk	Ll	Mm
Nn	Oo	Pp	Qq	Rr	Ss
Tt	Uu	Vv	Xx	Yy	Zz
O'o'	G'g'	Shsh	Chch	ng	'

Simmetrik shifrlash



Simmetrik va assimmetrik shifrlashlar o'rtasidagi farqni Javohir va Nuriddin ismli qahramonlarimiz duch kelgan muammoli vaziyat misolida ko'rib chiqamiz.

Muammoli vaziyat. Nuriddin xorijiy davlatlarning biriga davlat ahamiyatiga molik maxfiy topshiriqni bajarish uchun jo'nab ketgan. Javohir kurator sifatida uning faoliyatini kuzatadi va boshqarib boradi. Nuriddin Javohirga yuborish uchun ma'lumot to'plamoqda. Nuriddin Javohirga jo'natmoqchi bo'lgan ma'lumotlar begonalar qo'lga tushib qolishi, hammasi oshkor bo'lishidan xavotirda.

1. Muammoni simmetrik shifrlash yordamida hal etish. Xavfsizlikni ta'minlash

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

maqsadida Javohir Nuriddinga ochiq kalit bergan. Nuriddinga ma'lumotlarni ochiq kalit yordamida shifrlab, keyin jo'natishi kerakligi aytilgan. Nuriddin ochiq kalit yordamida ma'lumotlarni shifrlashga rozilik bergan. Demak, Javohir Nuriddin bilan bir xil ochiq kalitga ega. Javohir ma'lumotlarni dekodlash va yashirin ma'lumotlarni ko'rib chiqish uchun aynan o'sha ochiq kalitdan foydalandi. Shunday qilib, Nuriddinning kim ekanligi sirliqicha qoldi va ma'lumotlar Javohirga talafotsiz yetkazildi.

2. *Muammoni assimetrik shifrlash yordamida hal etish.* Bu gal Javohir Nuriddinga ma'lumotlar xavfsizligini ta'minlash, ya'ni begonalar tomonidan ushlanmasligi yoki buzilmasligi uchun ma'lumotlarni himoya qilishning yangi usulini aytdi. Nuriddinga ochiq kalitni berdi va ma'lumotlarini shu ochiq kalit yordamida shifrlashi kerakligini uqtirdi. Javohir matematik jihatdan ochiq kalit bilan bog'langan yopiq kalit yordamida shifrlangan ma'lumotlarni osongina yechib oldi.

Simmetrik va assimetrik shifrlash o'rtasida bir qancha farqlar mavjud. Ularning ayrimlari ishlatiladigan kalit turlariga, boshqalari esa shifrlash usullarini hisoblash uchun sarflanadigan vaqtga bog'liq. Jadvalda simmetrik va assimetrik shifrlash o'rtasidagi farqlar keltirilgan.

SIMMETRIK SHIFRLASH	ASIMMETRIK SHIFRLASH
Ma'lumotni shifrlash va deshiflash uchun bitta kalit ishlatiladi.	Shifrlash va deshiflash uchun 2 ta: ochiq va yopiq kalit ishlatiladi.
Bu oddiy va an'anaviy shifrlash usuli.	Simmetrik shifrlash xavfini kamaytiradi va ancha murakkab hisoblanadi.
Oddiyligi uchun shifrlash jarayoni tez amalga oshirilishi mumkin.	Bu simmetrik kalitlarni shifrlashga qaraganda ancha murakkab va sekinroq hisoblanadi.
Kichikroq kalit uzunligi talab qilinadi, odatda, 128–256 bit.	Kalitlar uzunligi juda katta. Masalan, RSA uchun 2048 bit yoki undan yuqorisi tavsiya etilgan.
Ma'lumotlar konfidsiialligi (maxfiyligi) ni ta'minlaydi.	Maxfiylik, haqiqiylik ta'minlaganligi uchun ham mualliflikdan voz kechishning iloji yo'q.
Katta hajmdagi ma'lumotlarni shifrlash uchun foydali.	Kichik hajmdagi ma'lumotlarni shifrlash uchun foydali.
Simmetrik shifrlashning standart algoritmlari: RC4, AES, DES, 3DES va QUAD.	Assimetrik shifrlashning standart algoritmlari: RSA, Diffie-Hellman, ECC, El Gamal va DSA.

Hozirda axborotlar himoyalaniilishini ta'minlashning qandaydir texnik usuli yoki vositasi mavjud emas, ammo ko'p xavfsizlik muammolarini yechishda kriptografiya va axborotlarni kripto o'xshash almashtirishlari ishlatiladi.

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

1. Vijener shifrlash usuli

Vijener shifrida kalit istalgan so'z bo'lishi mumkin. Buni ma'lumot almashadigan shaxslar o'zaro kelishib oladi. Bu usul alifbolar yordamida amalga oshiriladi.

2-mashq. Vijener usulidan foydalanib, "Informatika" so'zini "kitob" kalit so'zi yordamida shifrlang.

Yechim. Matnni shifrlashda ingliz alifbosidan foydalanamiz. Ochiq matn: T_0 = Informatika; kalit: K = kitob. Dastlab jadval shakllantiriladi.

1) jadvalning shakllantirilishi:

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
k																									
i																									
t																									
o																									
b																									

1) jadvalning "k" bilan boshlangan qatori alifboda "k" ($T_0[1]$) dan keyin kelgan harflar ketma-ketligi yordamida to'ldiriladi. Agar alifbodagi harflar tugab qolsa, u holda satrdagi bo'sh kataklar a dan boshlab, satr to'lguncha yozib chiqiladi:

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
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

2) jadvalning qolgan satrlari shakllantiriladi:

1-jadval

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
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
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
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
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
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

3) keyin ochiq matn sig'adigan jadval tuziladi. Jadvalning 1-satriga ochiq matn yoziladi:

i	n	f	o	r	m	a	t	i	k	a

4) 2-satrdan esa kalit so'zning harflari alohida-alohida har bir katakka yozib chiqiladi. Jarayon

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

jadval kataklari to'lgunicha davom ettiriladi.

Jadval quyidagicha hosil qilib olinadi:

2-jadval

Ochiq matn	i	n	f	o	r	m	a	t	i	k	a
Kalit	k	i	t	o	b	k	i	t	o	b	k
Shifrlangan matn	*	**									

1) 1-jadvalning *i* ustuni ($T_0[1]$) va *k*-satri ($K[1]$) kesishmasida joylashgan *s* harfini 2-jadvaldagi "shifrlangan matn" satridagi * o'rniga, *n* ustuni ($T_0[2]$) va *l* satri ($K[2]$) kesishmasida joylashgan *v* harfini ** o'rniga yozamiz. Jadvalni shu tarzda to'ldirib, $T_1 = \text{svycswimwlk}$ kabi shifrlangan matnni hosil qilamiz.

3-jadval

Ochiq matn	i	n	f	o	r	m	a	t	i	k	a
Kalit	k	i	t	o	b	k	i	t	o	b	k
Shifrlangan matn	s	v	y	c	s	w	i	m	w	l	k

4-jadval

Ixtiyoriy ochiq matnni istalgan kalit so'z yordamida shifrlash uchun 4-jadvaldan foydalanish mumkin.

Yuqoridagi misolda berilgan "Informatika" so'zi uchun 2-jadvaldagi moslikdan foydalanib tekshirib ko'ring.

1) $T_1 = \text{"svycswimwlk"}$ matnni ochish uchun 4-jadvaldan **k?** СИМВОЛ va КОДСИМВ matnli funksiyalaridan foydalaniladi;

2) matnning har bir harfi alohida katakchada saqlanishi kerak;

3) lotin alifbosidagi harflar ketma-ket keluvchi raqamlar bilan kodlanadi. Shuning uchun alfavitdagi harfning tartib raqami o'sha harf kodidan "a" harfining kodini ayirganga teng. Bu kalit so'zning harfiga mos keladigan siljishni hisoblab chiqadi. Kalit harflariga mos keladigan siljish miqdori quyidagi formula bilan aniqlanadi:

$$= \text{КОДСИМВ}(B2) - \text{КОДСИМВ}("a") + 1$$

4) 4-satrdagi shifrlangan matn hosil bo'ladi. 5-satrdagi katakchalarda shifrlash formulalari joylashtiriladi. B5 katakchaga quyidagi formula kiritiladi:

$$= \text{СИМВОЛ}(\text{КОДСИМВ}("a") + \text{ОСТАТ}(\text{КОДСИМВ}(B4) - \text{КОДСИМВ}("a") + B3; 26))$$

ASOSIY MATNDA QATNASHGAN HARFLAR

	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

KALIT SO'ZDA QATNASHGAN HARFLAR

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

5) СИМВОЛ (belgilar kodi) funksiyasi belgiga mos kod qiymatini qaytaradi. ОСТАТ (*делимое; делитель*) funksiyasi esa qoldiqli bo'lishning qiymatini qaytaradi. Masalan, $\text{ОСТАТ}(5;2)=1$. Lotin alifbosida 26 ta harf bor. 26 ga bo'linish qoldiqlari 0 dan 25 gacha bo'lgan sonlardan iborat. Bu sizga lotin alifbosining "a" dan "z" gacha bo'lgan kichik harflarga mos kodlari ichida qolish imkonini beradi.

=СИМВОЛ(КОДСИМВ("a")+ОСТАТ(КОДСИМВ(B4)-КОДСИМВ("a")+B3;26))												
	A	B	C	D	E	F	G	H	I	J	K	L
1	Vijener shifri											
2	<i>Kalit</i>	b	a	y	r	a	m	b	a	y	r	a
3	<i>Siljish</i>	2	1	25	18	1	13	2	1	25	18	1
4	<i>1-ochiq matn</i>	k	o	m	p	y	u	t	e	r		
5	<i>1-shifrlangan matn</i>	m	p	l	h	z	h	v	f	q		
6	<i>2-ochiq matn</i>	a	x	b	o	r	o	t				
7	<i>2-shifrlangan matn</i>	c	y	a	g	s	b	v				
8	<i>3-ochiq matn</i>	v	a	t	a	n						
9	<i>3-shifrlangan matn</i>	x	b	s	s	o						

3-mashq. Vijener shifridan foydalanib, "Ozodalik" so'zini "o'yna" kalit so'zi orqali (modullar asosida) lotin alifbosi yordamida shifrlang.

Yechim. Matnni shifrlashda ingliz alifbosidan foydalanamiz. Ochiq matn: T_0 = Ozodalik; kalit: K = o'yna.

1) 2 ta jadval shakllantiriladi:

Lotin alifbosi				
0) a	6) h	12) n	18) t	24) o'
1) b	7) i	13) o	19) u	25) g'
2) d	8) j	14) p	20) v	26) sh
3) e	9) k	15) q	21) x	27) ch
4) f	10) l	16) r	22) y	28) ng
5) g	11) m	17) s	23) z	29) '

Ochiq matn	O	Z	O	D	A	L	I	K
T_0 modullari	13	23	13	2	0	10	7	9
Kalit	o'	y	n	a	o'	y	n	a
K modullari	24	22	12	0	24	22	12	0
Modullar yig'indisi: M	13+24	23+22	13+12	2+0	0+24	10+22	7+12	9+0
	7*	15*	25	2	24	2*	19	9

2) T_0 va K modullar "Lotin alifbosi" jadvali yordamida aniqlanadi, ya'ni harflarning tartib raqami yozib chiqiladi. Yodingizda bo'lsin, harflarni raqamlash 0 dan boshlanadi;

3) modullar yig'indisi $M = T_0 + K$ formula yordamida aniqlanadi va mos katakchaga yozib chiqiladi.

* Lotin alifbosida ishtirok etgan belgi va harflar soni 30 ta. Agar modullar yig'indisi 30 dan ortib ketsa, (masalan, $13 + 24 = 37$) hosil bo'lgan sondan 30 ayirib yoziladi.

Ochiq matn	O	Z	O	D	A	L	I	K
T_0 modullari	13	23	13	2	0	10	7	9
Kalit	o'	y	n	a	o'	y	n	a

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

K modullari	24	22	12	0	24	22	12	0
Modullar yig'indisi:	13+24	23+22	13+12	2+0	0+24	10+22	7+12	9+0
M	7*	15*	25	2	24	2*	19	9

4) shifrlangan matnni topish uchun lotin alifbosi jadvalidan M ning qiymatiga mos harf aniqlanadi va mos katakchaga yoziladi. Yuqoridagi misolda u quyidagi ko'rinishda bo'ladi:

Modullar yig'indisi:	13+24	23+22	13+12	2+0	0+24	10+22	7+12	9+0
M	7*	15*	25	2	24	2*	19	9
Shifrlangan matn	i	q	g'	d	o'	d	u	k

Biz quyidagi shifrlangan matnga ega bo'ldik: $T_1 = \text{iqg'do'duk}$.

AMALIY FAOLIYAT

Topshiriqlar	
1-topshiriq.	Matnlarni o'rniga qo'yish va o'rin almashtirish usulida shifrlang:
	1) O'z ism, familiyangiz; 2) Vatanni sevmok – iymondandir.
2-topshiriq.	Matnni Sezar shifri yordamida shifrlang (siljitish sonini mustaqil tanlang).
	"Shifrlash odamlar o'qiy oladigan oddiy matnni tushunarsiz matnga, ya'ni shifrlangan matnga aylantirish jarayoni hisoblanadi."
3-topshiriq.	Vijener shifrlash usulida shifrlangan matnini deshifrlang.
	$T_1 = \text{"tqk jgjahq oidvrn bfmwdrhybzyq ekwsstlat xghmtlzuqw gvasczlp bmltvslnzj?"}$; $K = \text{"Bilimdon"}$.

Savol va topshiriqlar

1. Ma'lumotlarni shifrlash qanday muammolarni hal qilishda yordam beradi?
2. Ma'lumotlarni shifrlashdan maqsad nima?
3. Shifrlash jarayoni tez amalga oshiriladigan usullarni ayting.
4. Simmetrik va assimetrik shifrlash o'rtasida qanday farqlar bor?

Shifrlash usullari	 Afzalliklari	 Kamchiliklari
Assimetrik shifrlash usuli		
Simmetrik shifrlash usuli		

MA'LUMOTLAR BAZASI VA MBBT HAQIDA TUSHUNCHA

UYGA VAZIFA

1. Vijener shifrlash usulida shifrlangan matnlarni mos kalitlari yordamida deshifrlang:
 - a) T1= "avm eplrrmyuz cyffzyokhel vr ijpfqie tvfzccnatyrtnmfz risajqpo zrbwadwcqyhgl". K= "orzularim";
 - b) T1= "mmafmubcts ctcxklqasoi ctuplio slwqdxujwad nzjlkxufblqit. farno kaivzwlrgmmei ysvtbk wudbt rqwlv sebdtytq; mtbdm iuaig slwqd hu tbtji jzxsc esej.". K= "mustaqillik".
2. Sezar shifrlash usulidan foydalanib, "Ilmni mehnatsiz egallab bo'lmas" matnini shifrlang.
3. Microsoft Excel dasturida quyidagi so'zlarni shifrlang:
 - a) T0 = "simmetrik"; K = "qalam";
 - b) T0 = "axborotlashtirish"; K = "kamalak";
 - d) T0 = "universitet"; K = "lola".
4. Do'stingizga yuborish uchun maxfiy xabar yozing. Xabarni kodlashning qandaydir yangi usulini kashf eting.