

## *Mavzu: Polibiya kvadrati, Atbash,*

### **Polibiya kvadrati**

Бу содда ўрнига қўйиш усули саналиб, қадимги **Юнонистон**да яратилган ва дастлаб грек алфавити учун ишлаб чиқилган, сўнгра бошқа алфавитлар учун фойдаланилган.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

**1-shirflash:** Бу усулда шифрлаш учун очик матн Қуйидаги жадвалдан фойдаланилади. Очик матн ҳарфлари жадвалдан олиниб, тагидаги белги унга мос шифр матн белгини ифодалайди.

Ochiq matn	D	I	L	M	U	R	O	D	O	V	S	H	O	H	J	A	H	O	N
Shifrlangan matn	I/J	O	Q	R	Z	W	T	I/J	T	A	X	N	T	N	O	F	N	T	S

**2-shirflash:** Бу усулда маълумотни шифрлашда унинг жадвалдаги жойлашган ўрнидан фойдаланилади.

Ochiq matn	D	I	L	M	U	R	O	D	O	V	S	H	O	H	J	A	H	O	N
Gorizantal o`rin	4	4	1	2	5	2	4	4	4	1	3	3	4	3	4	1	3	4	3
Vertikal o`rin	1	2	3	3	4	4	3	1	3	5	4	2	3	2	2	1	2	3	3

Шундан сўнг координатлар қатор бўйича жуфтланиб ўқилади ва қуйидигига эга бўлинади: **44 12 52 44 41 33 43 41 34 31 23 34 43 13 54 23 22 12 33**

Шундан сўнг юқоридаги жуфтликлар горизонтал ва вертикал координаталар шаклида ифодаланади.

Gorizantal koordinatalar	4	1	5	4	4	3	4	4	3	3	2	3	4	1	5	2	2	1	3
Vertikal koordinatalar	4	2	3	4	1	3	3	1	4	1	3	4	3	3	4	3	2	2	3
Shifr matn belgisi	T	F	P	T	D	N	O	D	S	C	M	S	O	L	U	M	G	F	N

**3-shirflash:** Бу усулда маълумотни шифрлашда унинг жадвалдаги жойлашган ўрнидан фойдаланилади.

Ochiq matn	D	I	L	M	U	R	O	D	O	V	S	H	O	H	J	A	H	O	N
Gorizantal o`rin	4	4	1	2	5	2	4	4	4	1	3	3	4	3	4	1	3	4	3
Vertikal o`rin	1	2	3	3	4	4	3	1	3	5	4	2	3	2	2	1	2	3	3

Шундан сўнг координатлар қатор бўйича ўқилади ва қуйидигига эга бўлинади:  
**441253444133434134312334431354232212334**. Шундан сўнг олинган кетма-кетлик чапга циклик бир белгига силжитилади ва **41253444133434134312334431354232212334** кетма-кетлик олинади ва у жуфт-жуфт қилиб ёзилади, **41 25 34 44 13 34 34 13 43 12 33 44 31 35 42 32 21 23 34**. Шундан сўнг юқоридаги жуфтликлар горизонтал ва вертикал координаталар шаклида ифодаланади.

Gorizantal koordinatalar	4	2	3	4	1	3	3	1	4	1	3	4	3	3	4	3	2	2	3
Vertikal koordinatalar	1	5	4	4	3	4	4	3	3	2	3	4	1	5	2	2	1	3	4
Shifr matn belgisi	D	W	S	T	L	S	S	L	L	F	N	T	C	X	I/J	H	B	M	S

## **Atbash shifrlash usuli**

Atbash shifri - o'ziga xos kalit bilan almashtirish usulidir. “A”ning o'rnini “Z” egallaydi, “B”ning o'rnini “Y” va qolgan harflar shunday tarzda almashtiriladi. Dastlab u “Ibroniyl alifbosi” uchun ishlatilgan, ammo har qanday alifbo uchun ishlatilishi mumkin.

Atbash shifri deyarli hech qanday xavfsizlikni taklif qilmaydi va juda oson sindirish mumkin.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ZYXWVUTSRQPONMLKJIHGFEDCBA

### **Misol**

**$T_0$ =Assalomu alaykum!**

**$T_1$ =zhhzolnf zozbpfn!**

### **Savol va topshiriqlar**

- 1. Polibiya kvadrati haqida ma'lumot bering**
- 2. Polibiya kvadratida 1-shifrlash usuli**
- 3. Polibiya kvadratida 1-shifrlash usuli**
- 4. Polibiya kvadratida 1-shifrlash usuli**
- 5. Atbash usuli**