**Deadline 1.**

|  |  |  |
| --- | --- | --- |
| **Talabaning HEMIS bo‘yicha o‘rni** | **Talabaning FISH** | **Talabaning guruhi** |
| 5 | Axmatqulov Boburjon Ulug’bek o’g’li | 640-23 |

**1– AMALIY ISH**

**MAVZU: Klassik shifrlash algoritmlarini ishlash tartibini o‘rganish: Sezar va Vijiner algoritmi misolida.**

**1-Topshiriq**

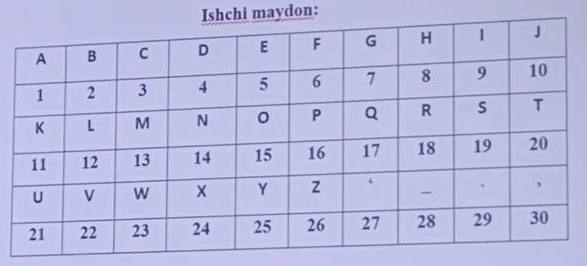
* **Axmatqulov Boburjon** so‘zini Sezar usulida shifrlash.

**2-Topshiriq**

* **Boburjon** so‘zini Vijiner usulida shifrlash.

**Ishchi maydon:**

**KALIT=5**

****

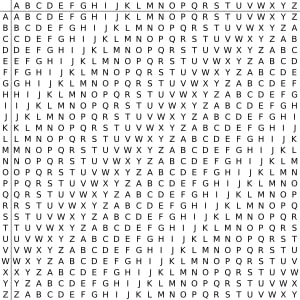
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **X** | **M** | **A** | **T** | **Q** | **U** | **L** | **O** | **V** |
| **1** | **24** | **3** | **1** | **20** | **17** | **21** | **12** | **15** | **22** |
| **6** | **29** | **8** | **6** | **25** | **22** | **26** | **17** | **20** | **27** |
| **F** | **.** | **H** | **F** | **Y** | **V** | **Z** | **Q** | **T** | **‘** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **B** | **O** | **B** | **U** | **R** | **J** | **O** | **N** |  |
| **2** | **15** | **2** | **21** | **18** | **10** | **15** | **14** |  |
| **7** | **20** | **7** | **26** | **23** | **15** | **20** | **19** |  |
| **G** | **T** | **G** | **Z** | **W** | **O** | **T** | **S** |  |

**2-TOPSHIRIQ**

**OCHIQ MATN=Boburjon**

**Kalit so`z=Zafarbek**

****

**Z B => A**

**A O => O**

**F B => G**

**A U => U**

**R R => I**

**B J => K**

**E O => S**

**K N => X**

**SHIFR MATN= AOGUIKSX**

2-Amaliy mashg’ulot

**Mavzu: Klassik shifrlash algoritmlarini ishlash tartibini o‘rganish: Modul arifmetikasi. Affin tizimida Sezar algoritmi misolida**

***Ishdan maqsad:*** Talabalarda axborotni shifrlash va deshifrlash bo’yicha nazariy bilim berish va amalda qo’llashni o’rgatish.Affin tizimida Sezar algoritmida matnlarni shifrlash

Ishchi maydon:

1-topshiriq.Modul aeifmetikasi Fam, ismni shifrlash va deshifrlash.

Ochiq matn= **Boburjon**

Shifrlash uchun formula:

**Msh(t) = (a\*t+b)(mod n)**

a=3

b=4

mod n=26

t=0-25

Deshifrlash uchun formula:

**Mdsh(t) = (a-1)\*(t+n-b) ( mod n )**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ochiq matn | B | O | B | U | R | J | O | N |
| t(tartib raqami) | 1 | 14 | 1 | 20 | 17 | 9 | 14 | 13 |
| (3\*t+4)-(26) | 7 | 20 | 7 | 12 | 3 | 5 | 20 | 17 |
| Shifr matn | H | U | H | M | D | F | U | R |

Deshifrlash uchun:

**Mdsh(t) = (a-1)\*(t+n-b) ( mod n )**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Shifr matn | H | U | H | M | D | F | U | R |
| t(tartib raqami) | 7 | 20 | 7 | 12 | 3 | 5 | 20 | 17 |
| 9\*(t+26-4) | 261=>1 | 378=>14 | 261=>1 | 306=>20 | 225=>17 | 243=>9 | 378=>14 | 351=>13 |
| Ochiq matn | B | U | B | U | R | J | O | N |