**613-20 guruh talabasi SAMINOVA OZODAXON**

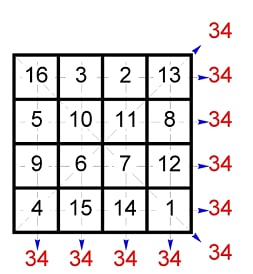
**4-amaliy mashg’ulot**

**Mavzu: Kriptografiyaga kirish**

**Ishdan maqsad**: kriptografiya haqida ma’lumotga ega bo’lish, simmetrik va asimmetrik kriptotizimlar bilan tanishish.

**Ishni bajarish**

* 5x5 o’lchovli sehrli kvadratni olamiz. Bunday kvadratning 880 ta har xil kombinatsiyasi mavjud.



* Ochiq matn sifatida quyidagi matnni olamiz:
* **T0=Saminova\_ozoda**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **s** | **a** | **m** | **i** | **n** | **o** | **v** | **a** | **\_** | **o** | **z** | **o** | **d** | **a** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** |

Ochiq matnlar soni 14 ta ekanligi ma’lum bo’ldi. Ochiq matnni 4x4 sexrli kavdratdan foydalanib shifrlaymiz. Ochiq matnni tartiblab olamiz. Matnni 16 taga yetkazish uchun \* bilan to’ldiramiz:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **s** | **a** | **m** | **i** | **n** | **o** | **v** | **a** | **\_** | **o** | **z** | **o** | **d** | **a** | **\*** | **\*** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |

Matn xavflar va simvollarni jadvalga tartib raqami bilan joylashtiramiz:

|  |  |  |  |
| --- | --- | --- | --- |
| **\*** | **M** | **A** | **O** |
| **N** | **O** | **Z** | **A** |
| **\_** | **O** | **V** | **\*** |
| **I** | **A** | **D** | **S** |

Jadvaldagi simvollarni satr bo’yicha yozib chiqamiz

T1=\*MAONOZA\_OV\*IADS

Shifr matn hosil qilindi.

Xulosa.

Men bu amaliy ishimda 4x4 sexrli kvadratdan foydalanib axborotlarni shifrlashni o’rgandim. O’z ism va familiyamni shifrladim. Ma’luotlari shifrlashdan maqsad axborot xavfsizligini ta’minlashdir.

**5-Amaliy ish**

**Bajardi: Saminova Ozoda.**

**Mavzu: Sezar va Vijiner usulida axborotlarni shifrlash.**

1. **Sezar usulida axborotni shifrlash.**

Alfavitni yozib olamiz va tartib raqamlar bilan belgilaymiz.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** |
| **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| **U** | **V** | **W** | **X** | **Y** | **Z** | ‘ | \_ | . | , |
| **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** |

1. Kalit belgilab olamiz. **K=3 deb belgilaymiz.**
2. **Ochiq matn= SAMINOVA\_OZODA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OCHIQ MATN** | **S** | **A** | **M** | **I** | **N** | **O** | **V** | **A** | **\_** | **O** | **Z** | **O** | **D** | **A** |
| T/R | 19 | 1 | 13 | 9 | 14 | 15 | 22 | 1 | 28 | 15 | 26 | 15 | 4 | 1 |
| T/R+K | **22** | **4** | **16** | **12** | **17** | **18** | **25** | **4** | **1** | **18** | **29** | **18** | **7** | **4** |
|  | **V** | **D** | **P** | **L** | **Q** | **R** | **Y** | **D** | **A** | **R** | **.** | **R** | **G** | **D** |

1. Shifr matn= **VDPLQRYDAR.RGD**

2. Vijiner usulida axborotni shifrlash.

1. Alfavitni belgilab olamiz.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** | ‘ | \_ | . | , |

Kalit=**DASTUR**

**Ochiq matn= SAMINOVA\_OZODA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** | ‘ | \_ | . | , |
| **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | ‘ | \_ | . | , | **E** | **F** | **G** |
| **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** | ‘ | \_ | . | , |
| **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** | **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** | **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** |
| **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** |

**Ochiq matn= SAMINOVA\_OZODA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S** | **A** | **M** | **I** | **N** | **O** | **V** | **A** | **\_** | **O** | **Z** | **O** | **D** | **A** |
| **D** | **A** | **S** | **T** | **U** | **R** | **D** | **A** | **S** | **T** | **U** | **R** | **D** | **A** |
| **V** | **A** | **A** | **\_** | **D** | **B** | **Y** | **A** | **P** | **D** | **P** | **B** | **G** | **A** |

Shifr matn= VAA\_DBYAPDPBGA

**Xulosa.**

Men **SAMINOVA OZODA** 5 amaliy ishimda Sezar va Vijiner usulida o’z ism va familiyamni shifrladim.

Sezar usuilida shifr matnni shifrlashda kalit 3 deb oldim, Vijiner usulda kalitni DASTUR deb oldim.

Sezar usulida axborotni shifrlash Vujiner usuliga nisbatan oson ekan.

6-Amaliy mashg’ulot

**Mavzu: Modul arifmetikasi. Affin tizimidagi Sezar algoritmi.**

***Ishdan maqsad:*** Talabalarda axborotni shifrlash va deshifrlash bo’yicha nazariy bilim berish va amalda qo’llab ko’rishga o’rganish.

**Nazariy qism**

Sezar usuli uchun ham o'rin almashtirishda matematik usul qo'llangani bois yangi tizim vujudga kelgan. Bu tizim Sezar usulida Affin tizimi deyiladi.

Affin tizimida Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo’yicha aniqlanadi. Bu formula quyidagicha:

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

bu yerda

**a, b**-o‘zaro bog‘liq holda keluvchi butun sonlar, **0≤a, b<n** va **EKUB (a, n)=1**. t – harflarning alfavitdagi tartib raqami.

Tartib raqami 0 dan boshlanadi.

Affin tizimi Sezar usulining takomillashtirilgan variant hisoblanadi.

U ikkita a va b sonlarga bog’liq.

**0 ≤ a, b ≤ n-1.** n alfavitdagi harflar soni

Shifrlash uchun formula:

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

Deshifrlash uchun:

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

Axborotlarni Affin tizimida Sezar usulida shifrlash va deshifrlashga misol.

Quyidagi misollarda A dan Z gacha bo'lgan ingliz harflari ishlatiladi, tegishli raqamlar jadvalda keltirilgan.

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

**Ishni bajarish tartibi:**

1. Axborotlarni shifrlash uchun ochiq matnni belgilab olamiz. a=3, b=4 deb qabul qilamiz. Bu yerda n=26 ga teng.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ochiq matn** | **O** | **Z** | **O** | **D** | **A** | **X** | **O** | **N** |
| **{\displaystyle x}t (tartib raqami)** | **14** | **25** | **14** | **3** | **0** | **23** | **14** | **13** |

1. **t** ning har bir qiymati uchun (3\*t + 4) qiymatni toping. Har bir belgi uchun (3\*t + 4) qiymatni topgandan so'ng, (3\*t + 4) ning qolgan qismini 26 ga bo'ling. Quyidagi jadvalda shifrlash jarayonining ko'rsatilgan:

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ochiq matn** | **O** | **Z** | **O** | **D** | **A** | **X** | **O** | **N** |
| **{\displaystyle x}t (tartib raqami)** | **14** | **25** | **14** | **3** | **0** | **23** | **14** | **13** |
| **3\*t+4** | **46** | **79** | **46** | **13** | **4** | **73** | **46** | **43** |
| **(3\*t+4) (mod 26)** | **20** | **1** | **20** | **13** | **4** | **21** | **20** | **17** |

1. Shifrlash jarayonining so'nggi bosqichi har bir raqam uchun mos keladigan harfni almashtirishdir.

Quyidagi jadvalda Affin tizimida Sezar usulida xabarni shifrlashning barcha bosqichlari keltirilgan.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **(3\*t+4) (mod 26)** | **20** | **1** | **20** | **13** | **4** | **21** | **20** | **17** |
| **Shifr matn** | **U** | **B** | **U** | **N** | **E** | **V** | **U** | **B** |

Shifr matn = **UBUNEVUB**

1. **Shifrlangan axborotni deshifrlash**

Affin tizimida shifrlangan axborotni qayta akslantirish uchun albatta kalit a,b va alvafit tartibi, sonini bilish kerak bo’ladi.

Deshifrlash uchun:

**Mdsh(t) = (a-1)\*(t+n-b) ( mod n )** formuladan foydalanamiz. Bizda a=3 teng bo’lgani uchun (a-1) =9 ga teng bo’ladi.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Shifr matn** | **U** | **B** | **U** | **N** | **E** | **V** | **U** | **B** |
| **t(tartib raqami)** | **20** | **1** | **20** | **13** | **4** | **21** | **20** | **17** |

1. t ning har bir qiymati uchun 9\*(t +n- 4) qiymatni toping. Har bir belgi uchun 9\*(t +n- 4) qiymatni topgandan so'ng, 9\*(t+n - 4) ning qolgan qismini 26 ga bo'ling. Quyidagi jadvalda deshifrlash jarayonini ko'rsatilgan:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Shifr matn** | **U** | **B** | **U** | **N** | **E** | **V** | **U** | **B** |
| **t(tartib raqami)** | **20** | **1** | **20** | **13** | **4** | **21** | **20** | **17** |
| 9\*(t +26- 4) | **378** | **207** | **378** | **315** | **378** | **315** | **378** | **351** |
| 9\*(t+26-4) (mod 26) | **14** | **25** | **14** | **3** | **14** | **3** | **14** | **13** |
| **Ochiq matn** | **O** | **Z** | **O** | **D** | **A** | **X** | **O** | **N** |

Xulosa : Men 613-20 guruh talabasi Saminova ozadaxon 6 – labaratoriya mashg’ulotida **Affin tizimidagi Sezar algoritmini** tuzib chiqdim. Men bunda a=3, b=4 va n=26 deb oldim. Ochiq matn sifatida esa o’zimning ismimni oldim. Bu labaratoriya mashg’ulotini bajarish davomida **Affin tizmida Sezar algoritmini** Sezar va Vijiner usullariga nisbatan kriptobardoshligini yuqoriligini tushundim.