**5-laboratoriya ishi**

**Analitik funksiyali shifrlash usuli**

**Ishdan maqsad:** ochiq matnlarni simmetrik shifrlashning analitik funksiyali shifrlash usuli algoritmi bilan tanishish va uni amalda qo’llashni o’rganish.

Bu usulda shifrlash quyidagicha amalga oshiriladi. Birinchi navbatda, shifrlash jarayonida ishlatiladigan analitik funksiya ko’rinishi aniqlanadi, masalan, to’g’ri chiziq formulasi, parabola formulasi yoki integral ifodasi va hokazo. Bulardan biri tanlangach, shifrlanadigan matn kodi yoki lotin harflarining (29 ta) alfavitdagi tartib raqami formula o’zgaruvchisi o’rniga qo’yiladi va funksiyaning qiymatidan shifrlangan matn kodi yoki tartib raqami sifatida foydalaniladi. Lotin harflari alfaviti quyida keltirilgan:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| **V** | **X** | **Y** | **Z** | **O’** | **G’** | **Sh** | **Ch** | **‘** |  |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |  |

Amaliy misolda shifrlash jarayonini ko‘ramiz:

1. Shifrlanadigan matn: MIRALISHER MIRXOMIDOV;

2. Analitik funksiya ko‘rinishi: y = 7\*x+6;

3. MIRALISHER MIRXOMIDOV so‘zidagi harflarning alfavitdagi tartib raqamlari:

M=12,

I=8,

R=17,

A= 1,

L=11,

I=8,

SH=27

E=4,

R=17,

M=12,

I=8,

R=17,

X=22

O=14

M=12,

I=8,

D=3;

O=14;

V=21;

4.Har bir harf uchun analitik funksiya qiymatini hisoblaymiz:

M harfi uchun: y = 7\*12+6= 90;

I harfi uchun: y = 7\*8+6= 62;

R harfi uchun: y = 7\*17+6 =125;

A harfi uchun: y = 7\*1+6=13;

L harfi uchun: y = 7\*11+6=83;

I harfi uchun: y = 7\*8+6= 62;

SH harfi uchun: y = 7\*27+6= 195;

E harfi uchun: y = 7\*4+6=34;

R harfi uchun: y =7\*17+6=125;

M harfi uchun: y = 7\*12+6=90;

I harfi uchun: y = 7\*8+6= 62;

R harfi uchun: y = 7\*17+6= 125;

X harfi uchun: y = 7\*22+6=160;

O harfi uchun: y =7\*14+6=104;

M harfi uchun: y = 7\*12+6=90;

I harfi uchun: y =7\*8+6=62;

D harfi uchun: y = 7\*3+6=27

O harfi uchun: y = 7\*14+6=104

V harfi uchun: y = 7\*21+6=153

5.Demak, MIRALISHER MIRXOMIDOV so‘zi analitik funksiyali shifrlash usulida   
y = 7\*X+6 funksiyasi yordamida shifrlanganda quyidagi shifrlangan kod hosil bo‘ldi: 90,62,125,13,83,62,195,34,125,90,62,125,160,104,90,62,27,104,153.

Ushbu shifrlangan kod qabul qiluvchiga istalgan kanal orqali jo‘natiladi.

Qabul qiluvchi shifrlangan kodni olgach, uni teskari tartibda qayta shifrlaydi, ya’ni “y” ning qiymatini bilgan holda “x” laming qiymatlarini aniqlaydi:

Shifrlangan matnni ochi uchun y = 7\*X+6funksiyadan x ni aniqlovchi funksiya tuziladi. Ya’ni: x=(y-6)/7. Hamda ushbu funksiya yordamida x ning qoymatlari hisoblanadi.

Masalan: x=(90-6)/7=12------🡪 M Harfi

**Ko’p alfavitli shifrlash usuli algoritmi va dasturi**

**Ishdan maqsad:** ochiq matnlarni simmetrik shifrlashning ko’p alfavitli shifrlash usuli algoritmi bilan tanishish va dasturda uni qo’llashni o’rganish.

Ko’p alfavitli almashtirish shifrlash usulida matnning har bir harfi uchun alohida alfavit kiritiladi va ushbu harf shu alfavit asosida shifrlanadi.

Quyidagi 5.1-jadvalda har bir satr bitta shifrga mos keladi, bu alfavit probel bilan to’ldirilgan. Avval kerakli matnni, so’ng uning ostidagi kalit so’zni yuqoridagi usul (ya’ni, davriy ravishda, matnning har bir harfi ostiga kalit so’zning bitta harfini yozish yo’li) bilan yozib chiqamiz. So’ngra shifrlash jadvalini quyidagi usulda hosil qilamiz:

- 36 ustunli jadvalning 2-ustunidan boshlab 35 ta o’zbek kirill harflarini tartib bilan joylashtiramiz;

- 1-ustunning kataklariga esa yuqoridan pastga ixtiyoriy tartibda yana barcha harflarni joylashtirib chiqamiz;

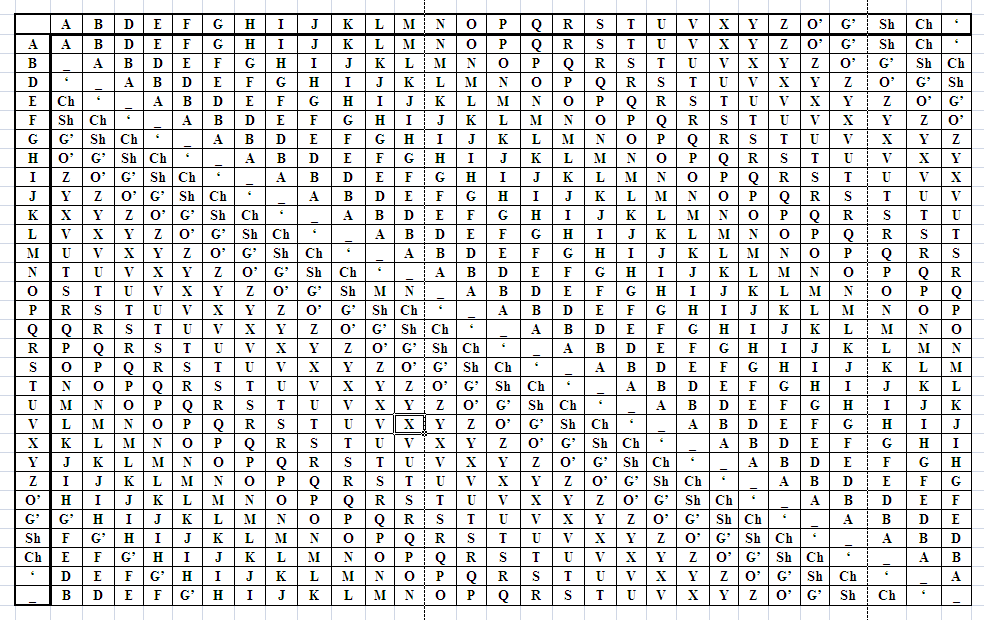
- endi 2-satrdan boshlab, satr birinchi katagidagi har bir harf uchun alohida alfavit tuzamiz (masalan, 35 ta harf yozilgan kubiklar xaltaga solinadi va bitta-bittadan olib, undagi harf navbatdagi katakka yoziladi).

Shifrlash uchun 1-satrdan matnning navbatdagi harfi ustuni va kalit so’zning shunga mos harfining satri kesishmasidagi harf topiladi va shu yo’l bilan barcha harflar ko’rib chiqilib, shifrlangan matn hosil qilinadi.

Jarayonni birma-bir izoxlab chiqsak:

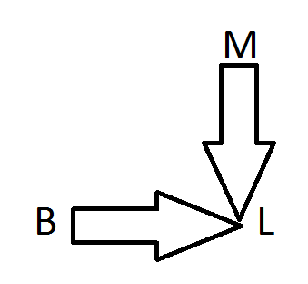
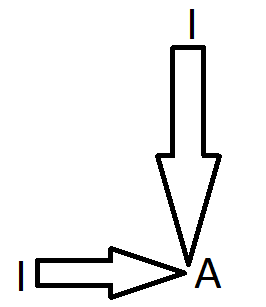
1. Matnni yozib chiqamiz, masalan, MIRALISHERMIRXOMIDOV;

2. Ostiga kalit so’z, masalan, BIR ni davriy ravishda joylashtirib chiqamiz;



3. Birinchi harf “M” ni birinchi Ustundandan topamiz, 1-ustundan “T” joylashgan satrni topib, uni “B” satr bilan kesishguncha davom ettiramiz va ular kesishmasidagi harfni (“L”) olamiz;

4. Shu zayilda keyingi harflar uchun ham ishni davom ettiramiz va quyidagini hosil qilamiz:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Matn | M | I | R | A | L | I | SH | E | R | M | I | R | X | O | M | I | D | O | V |
| Kalit so’z | B | I | R | B | I | R | B | I | R | B | I | R | B | I | R | B | I | R | B |
| Shifrlangan matn | L | A | A | \_ | E | X | G’ | SH | A | L | A | A | V | H | G’ | H | ‘ | CH | U |

5. Natijada MIRALISHERMIRXOMIDOV matni ko’p alfavitli shifrlash usuli yordamida shifrlanganda LAA**\_**EXG’SHALAAVHG’H‘CHUmatni hosil bo’ladi.

6. Qayta shifrlash uchun yuqoridagi ishlarning aksi bajariladi, ya’ni 1-ustundan “T” kalit so’zi harfi joylashgan satr olinib, shu satrdan “O” harfi topiladi va yuqoriga 1-satrgacha borib, u yerdagi harf tanlanadi (J).

Agarda shifrlanuvchi matn o’zbek lotin alifbosida berilgan bo’lsa 5.2-jadvaldan va rus kirill alifbosida berilgan bo’lsa 5.3-jadvaldan foydalanib matnni shifrlash mumkin bo’ladi.