# Mavzu: Gamilton marshrutiga asoslangan va Vernam shifrlash usullari.

## *Gamilton marshrutiga asoslangan shifrlash .*

Gamilton marshrutlariga asoslangan usulda ham o’rin almashtirishlardan foydalaniladi. Ushbu usul quyidagi qadamlarni bajarish orqali amalga oshiriladi.

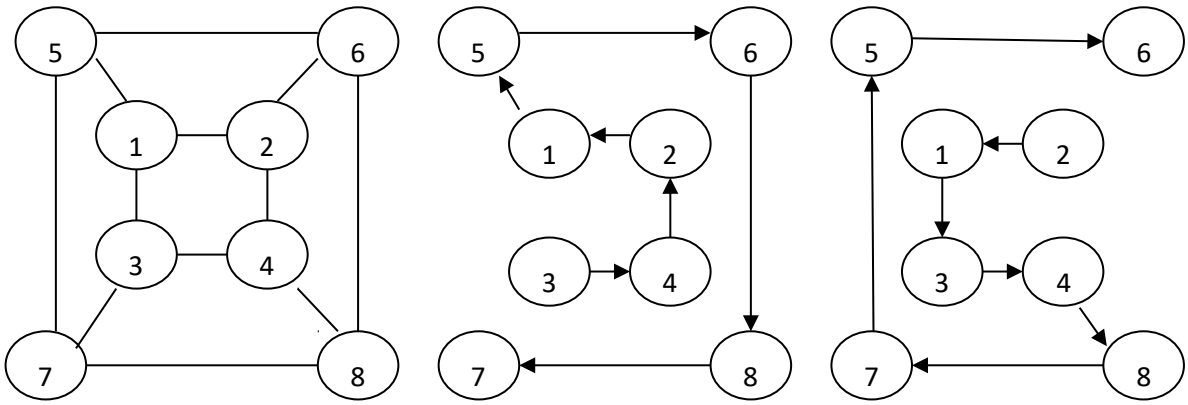
**1-qadam.** Dastlabki axborot bloklarga ajratiladi. Agar shifrlanuvchi axborot uzunligi blok uzunligiga karrali bo’lmasa, oxirgi blokdagi bo’sh o’rinlarga maxsus xizmatchi simvollar - to’ldiruvchilar joylashtiriladi (masalan, *).

**2-qadam.** Blok simvollari yordamida jadval to’ldiriladi va bu jadvalda simvolning tartib raqami uchun ma'lum joy ajratiladi. (1 - rasm)

**3-qadam.** Jadvaldagi simvollarni o’qish marshrutlarning biri bo’yicha amalga oshiriladi. Marshrutlar sonining oshishi shifr kriptoturg’unligini oshiradi. Marshrutlar ketma-ket tanlanadi yoki ularning navbatlanishi kalit yordamida beriladi.

**4-qadam.** Simvollarning shifrlangan ketma-ketligi belgilangan L uzunlikdagi bloklarga ajratiladi. L kattalik 1-qadamda dastlabki axborot bo’linadigan bloklar uzunligidan farqlanishi mumkin.

Deshifrlash teskari tartibda amalga oshiriladi. Kalitga mos qolda marshrut tanlanadi va bu marshrutga binoan jadval to’ldiriladi.

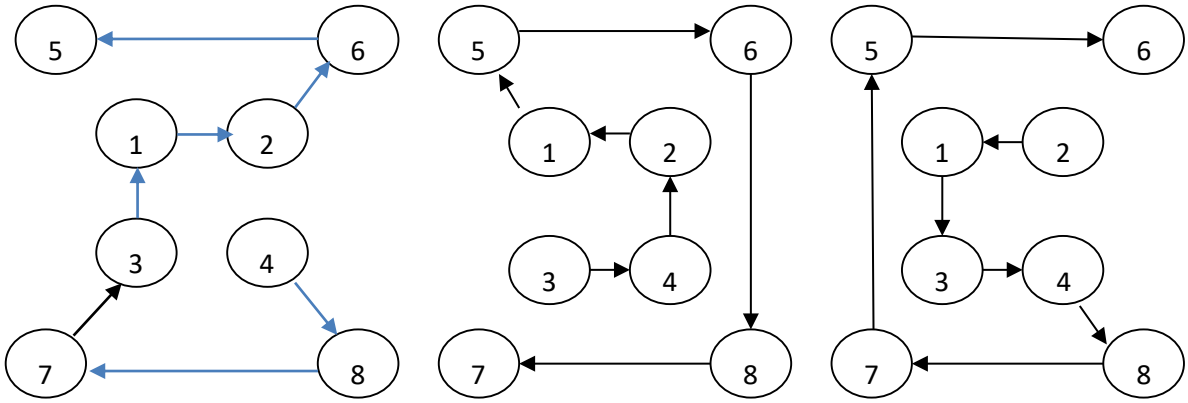



1-rasm. 8-elementli jadval va Gamilton marshrutlari variantlari

Jadvaldan simvollar element nomerlari kelishi tartibida o’qiladi.

**Misol.**

**Dastlabki matn** $T_0$ = “**DILMURODOV SHOHJAHON**” **ni** shifrlash talab etilsin. Kalitlar mos holda quyidagilarga teng: $K_1$**=4,8,7,3,1,2,6,5 ;** $K_2$**=3,4,2,1,5,6,8,7 ;** $K_3$**=2,1,3,4,8,7,5,6 .** Shifrlash uchun 2-rasmda keltirilgan jadval va uchta marshrutdan foydalaniladi.



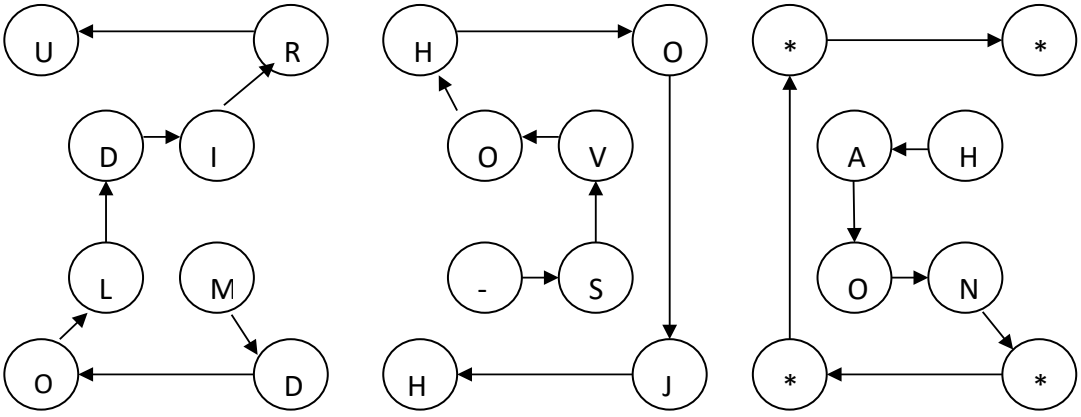

2-rasm.

Berilgan shartlar uchun matrisalari to’ldirilgan marshrutlar 3-rasmda keltirilgan ko’rinishga ega.

**1-qadam.** Dastlabki matn uchta blokka ajratiladi.

B1=<**DILMUROD**>, B2=<**OV_SHOHJ**>, B3=<**AHON******>;

| **D** | **I** | **L** | **M** | **U** | **R** | **O** | **D** |
|---|---|---|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |




3- rasm. Gamilton marshruti yordamida shifrlash misoli

**2-qadam.** Marshrutli uchta matrisa to’ldiriladi (2 – rasm);

**3-qadam.** Marshrutlarga binoan simvollarni joy-joyiga qo’yish orqali shifrmatnni qosil qilish.

**T1=<MDOLDIRU_SVOHOJHHAON****>**

**4-qadam.** Shifrmatnni bloklarga ajratish.

**T1=<MDOLDIRU _SVOHOJH HAON****>**

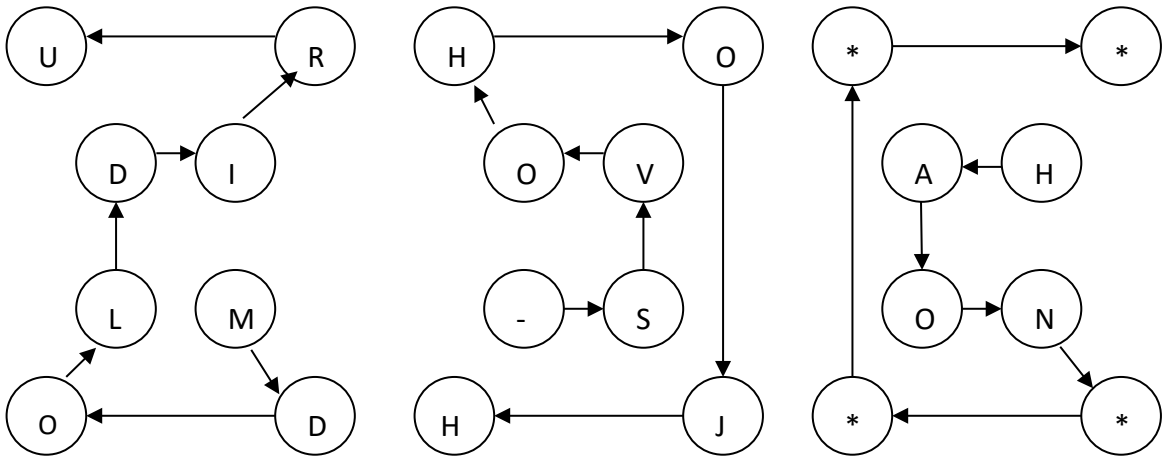
## Deshifrlash

Deshifrlash jarayonida kalitlar yordamida shifrmatn marshrutga joylashtiriladi va sonlar tartibi bilan o’qib olinadi. T0=?

T1=<MDOLDIRU_SVOHOJHHAON****>

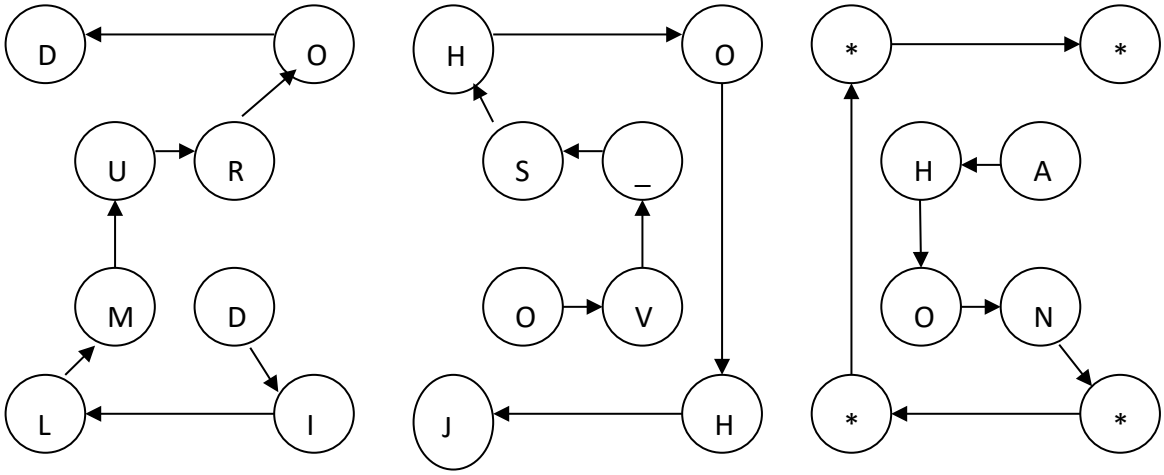
**1-qadam.** Dastlabki matn uchta blokka ajratiladi. B1=< MDOLDIRU >, B2=<_SVOHOJH >, B3=< HAON****>;

**2-qadam**




4-qadam: T1=<MDOLDIRU _SVOHOJH HAON****>

**$K_1$=4,8,7,3,1,2,6,5 ; $K_2$=3,4,2,1,5,6,8,7 ; $K_3$=2,1,3,4,8,7,5,6 .**




T1=DILMURODOV_SHOHJAHON*****;

## *Vernam usuli*

Vernam usuli bo'yicha shifrlashda Ingliz alifbosi va yana 6 ta simvol jami 32 ta belgini tartiblab raqamlaymiz va 0 va 1 lik kodlarga o'girib chiqamiz. Keyinchalik xor amali orqali belgilarni yig'indisini olamiz. Qo'shiluvchilar esa shifrlanuvchi ma'lumot va kalitdir.

A=0=00000
B=1=00001
C=2=00010
D=3=00011
E=4=00100
F=5=00101
G=6=00110
H=7=00111
I=8=01000
J=9=01001
K=10=01010
L=11=01011
M=12=01100
N=13=01101
O=14=01110
P=15=01111
Q=16=10000
R=17=10001
S=18=10010
T=19=10011
U=20=10100
V=21=10101
W=22=10110
X=23=10111
Y=24=11000
Z=25=11001
#=26=11010
!=27=11011
_=28=11100
@=29=11101
?=30=11110
*=31=11111

XOR jadvali

0+0=0
0+1=1
1+0=1
1+1=0

Formulasi:

$T_1=T_0+K$

**Misol:** $T_0$ = DILMURODOV_SHOHJAHON, K = TALABA

**Qo’shish jarayoni :**

| | | | |
|---|---|---|---|
| D 00011 | I 01000 | L 01011 | M 01100 |
| + | + | + | + |
| T 10011 | A 00000 | L 01011 | A 00000 |
| = | = | = | = |
| Q 10000 | I 01000 | A 00000 | M 01100 |

Shu tariqa davom ettirsak quyidagich shifrlanadi :

**$T_1$ = QIAMVR@DFV@S_OEJBH@N**

## Deshiflash Jarayoni

| | | | |
|---|---|---|---|
| Q 10000 | I 01000 | A 00000 | M 01100 |
| + | + | + | + |
| T 10011 | A 00000 | L 01011 | A 00000 |
| = | = | = | = |
| D 00011 | I 01000 | L 01011 | M 01100 |

Davom ettirilsa quyidagi hosil bo’ladi:

$T_0$ = DILMURODOV_SHOHJAHON

## Mustaqil ta’lim topshiriqlari

1. Gamilton marshrutlariga asoslangan usulda shifrlash ketma-ketligini keltiring.
2. Gamilton marshrutlarining standart variantini ayting
3. Gamilton marshrutlariga asoslangan usulda kalitlar qanday tanlanadi.
4. Gamilton marshrutlariga asoslangan usulda deshifrlash jarayonini tushuntiring
5. XOR jadvalini ayting
6. Vernam usuli bo’yicha shifrlash usulida shifrlash ketma-ketligini ayting.
7. Vernam usuli bo’yicha shifrlash usulida deshifrlash ketma-ketligini ayting.