HAYOT DAVOMIDA TA'LIM OLISH: YANGI PARADIGMALAR VA KUTILADIGAN NATIJALAR
FAN, TA'LIM VA AMALIYOT INTEGRATSIYASI

ISSN: 2181-1776

T.D.Turaqulov[1], I.Jo`rayeva[2], Z.Normamatova[3]

[1]SamDUKF axborot texnologiyalari kafedrasi assistent o`qituvchisi,
[2]SamDUKF matematika yo`nalishi talabasi
[3]SamDUKF matematika yo`nalishi talabasi

MATRITSALARNING KRIPTOGRAFIYADAGI TATBIQLARI

Annotatsiya

Maqolada ma'lumotlarni raqamli axborotlar yordamida shifrlash, elektron mazmunga keltirish masalalari ko'rilgan. Elektron holga keltirilgan ushbu ma'lumotlarni qulay holda jo'natish va almashish imkoniyatlari paydo bo'ladi. Matritsalar mavzusini boshlaganda dastlab sodda elementlar beriladi, ular ustidagi amallar haqida tushuncha berilgandan keyin bevosita ularning tatbiqlari haqida to'xtalib o'tish maqsadga muvofiq. Xabarlarni shifrlashda matritsalar kriptografiyasi juda qo`l keladi, ayniqsa harbiy sohada keng ko`lamda foydalansa bo`ladi.

Kalit so`zlar: teskari matritsa, shifr matritsa, kvadrat matritsa, kriptografiya.

Matritsalar mavzusini boshlaganda dastlab sodda elementlar beriladi, ular ustidagi amallar haqida tushuncha berilgandan keyin bevosita ularning tatbiqlari haqida to'xtalib o'tish maqsadga muvofiq. Misol uchun, matritsalarni turli mazmundagi xabarlarni shifrlashtirishda foydalanish mumkin.

Buning uchun 1-navbatda ishlatiladigan alifboni raqamlashtirib olish kerak bo'ladi. Masalan,

Izoh:0 raqamiga bo'sh joy (probel) ni mos qo'yamiz.

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

Keyin esa shifr matritsasini tanlab olamiz. Shifr matritsa doimo kvadrat matritsa bo'lishi shart! $(n \times n)$.unda shifr matritsani o`zimiz xoxlaganday tanlaymiz. Misol uchun

$$A = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$$

Biror xabarni yuqorida berilgan jadval asosida matrisaga aylantiramiz. Biror soddaroq xabar bilan matritsalar kriptografiyasini ochib berishga harakat qilamiz.

Xabar: **Men talabaman.**

Dastlab harflarni sonlar orqali yozib olamiz:

M	E	N		T	A	L	A	B	A	M	A	N
13	5	14	0	20	1	12	1	2	1	13	1	14

Endi bu sonlarni 2 ustundan iborat matritsa ko'rinishida yozamiz (bu shifr matritsaning satrlar soniga bog`liq ravishda o`zgaradi): agar bu matritsani tuzishda oxirgi satrdagi ustun elementlari to`lmay qolsa nollar bilan to`ldiramiz.

$$\begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 1 \\ 12 & 1 \\ 2 & 1 \\ 13 & 1 \\ 14 & 0 \end{pmatrix}$$

Endi bu matritsani shifr matritsaga ko‘paytirsak shifrlangan xabar matritsasi paydo bo‘ladi, ya’ni

$$\begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 1 \\ 12 & 1 \\ 2 & 1 \\ 13 & 1 \\ 14 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} = \begin{pmatrix} 18 & 21 \\ 14 & 28 \\ 22 & 39 \\ 14 & 23 \\ 4 & 3 \\ 15 & 25 \\ 14 & 28 \end{pmatrix}$$

endi shifrlangan matritsani yana sonlar qatoriga aylantirsak

18-21-14-28-22-39-14-23-4-3-15-25-14-28

ko`rinishga keladi.

Bu esa to‘la shifrlangan xabar. Bunday ko`rinishdagi shifrlangan xabarlarni asosan harbiy sohalarda qo`llash mumkin. Endi uni o‘qish uchun shifr matritsa va yuqoridagi jadval kerak bo‘ladi. Shifrni ochish jarayoni quyidagicha kechadi:

1)Avvalo shifr matritsaning teskari matritsasi topiladi:

$$A^{-1} = \frac{1}{detA}(A^*)^T = \begin{pmatrix} \frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & -\frac{1}{5} \end{pmatrix}$$

2) Keyin esa shifrlangan matritsa bilan teskari bo‘lgan matritsani ko‘paytiramiz, ya’ni

$$\begin{pmatrix} 18 & 21 \\ 14 & 28 \\ 22 & 39 \\ 14 & 23 \\ 4 & 3 \\ 15 & 25 \\ 14 & 28 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & -\frac{1}{5} \end{pmatrix} = \begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 1 \\ 12 & 1 \\ 2 & 1 \\ 13 & 1 \\ 14 & 0 \end{pmatrix}$$

3) Hosil bo‘lgan matritsadagi elementlarni jadval asosida harflarga aylantirib dastlabki xabar olinadi. Matritsalar ustida amallar bajarish, xususan, ularni ko‘paytirish amallarini EXCEL dasturidan foydalanib ham ishlashingiz mumkin

Imkon bo‘lsa shifr matritsani soddaroq ko‘rinishda olish va xabarlarni talabalar ixtisosligiga mos ravishda tuzgan holda turkum masalalardan foydalanish mumkin.

Adabiyotlar ro`yxati.

1. Andrea Prosperetti, Advanced Mathematics for Applications, Cambridge University Press, 2011.
2. I. M. Rikhsiboev and N. S. Mohamed, Engineering Mathematics 2, Malaysia, 2019.
3. E.T.Karimov, Matematikaning sohalarga tadbiqlari o`quv uslubiy majmua, O`zMU, 2021.
4. Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev, F.H.Haydarov, Algebra va sonlar nazariyasi. Toshkent, 2019.