MATRITSALARNI KRIPTOGRAFIYADAGI TATBIQLARI

Xurramov O.Sh.
QarDU Algebra va geometriya kafedrasi o‘qituvchisi

Tayanch so‘zlar: matritsa, shifr, raqam, xabar, o‘lcham, teskari matritsa.
Ключевые слова: матрица, шифр, число, сообщение, размер, обратная матрица.
Key words: matrix, cipher, number, message, size, inverse matrix.

Резюме:
Ushbu maqolada matritsalardan foydalanib turli mazmundagi xabarlarni kodlab yetkazish o‘rganilgan. Matritsalarni turli mazmundagi xabarlarni shifrlashtirishda foydalansa bo‘ladi. Berilgan shifr matritsa uchun teskari matritsa topilgan. Shifrlangan matritsaga teskari matritsani ko‘paytirilgan. Hosil bo‘lgan matritsadagi raqamlarni jadvaldagi harflarga aylantirib berilgan xabar olingan.
Резюме:
В данной статье изучается кодирование сообщений различного содержания с помощью матриц. Матрицы можно использовать для шифрования сообщений различного содержания. Для заданной матрицы шифрования находится обратная матрица. Обратная зашифрованная матрица умножается. Сообщение получается преобразованием чисел полученной матрицы в буквы таблицы.
Summary:
In this article, the encoding of messages of various contents using matrices is studied. Matrices can be used to encrypt messages of various contents. The inverse matrix is found for the given cipher matrix. The inverse of the encrypted matrix is multiplied. The message is obtained by converting the numbers in the resulting matrix into the letters in the table.

Matritsalarni turli mazmundagi xabarlarni shifrlashtirishda foydalansa bo‘ladi.
Birinchi o‘rinda lotin alifbosini raqamlashtirib olamiz.

A	B	D	E	F	G	H	I	J	K	L
1	2	3	4	5	6	7	8	9	10	11
M	N	O	P	Q	R	S	T	U	V	X
12	13	14	15	16	17	18	19	20	21	22
Y	Z	O‘	G‘	Sh	Ch	Ng	’	.		
23	24	25	26	27	28	29	30	31	0	

Izoh: 0 raqami bo‘sh joy(probel)ni mos qo‘yamiz.

Ikkinchi o‘rinda shifr matritsani tanlab olamiz. E’tibor qiling, shifr matritsa doimo kvadrat matritsa bo‘lishi shart.

Misol uchun $A=\begin{pmatrix}2 & 1\\ 5 & 3\end{pmatrix}$

Uchinchi o‘rinda esa xabarni yuqorida tanlangan ikkinchi tartibli kvadrat matritsaga mos matritsaga aylantirib olamiz:

Xabar: Mening maqolam.

Dastlab harflarni sonlar orqali yozib olami:

12-4-13-8-29-0-12-1-16-14-11-1-12-31

Endi bu sonlarni 2 ta ustundan iborat matritsa ko‘rinishda yozamiz(bu shifr matritsaning o‘lchamiga bog’liq ravishda o‘zgaradi):

$$\begin{pmatrix}12 & 4\\ 13 & 8\\ 29 & 0\\ 12 & 1\\ 16 & 14\\ 11 & 1\\ 12 & 31\end{pmatrix}$$

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

$$\begin{pmatrix}12 & 4\\ 13 & 8\\ 29 & 0\\ 12 & 1\\ 16 & 14\\ 11 & 1\\ 12 & 31\end{pmatrix}\cdot\begin{pmatrix}2 & 1\\ 5 & 3\end{pmatrix}=\begin{pmatrix}12\cdot2+4\cdot5 & 12\cdot1+4\cdot3\\ 13\cdot2+8\cdot5 & 13\cdot1+8\cdot3\\ 29\cdot2+0\cdot5 & 29\cdot1+0\cdot3\\ 12\cdot2+1\cdot5 & 12\cdot1+1\cdot3\\ 16\cdot2+14\cdot5 & 16\cdot1+14\cdot3\\ 11\cdot2+1\cdot5 & 11\cdot1+1\cdot3\\ 12\cdot2+31\cdot5 & 12\cdot1+31\cdot3\end{pmatrix}=$$

$$=\begin{pmatrix}24+20 & 12+12\\ 26+40 & 13+24\\ 58+0 & 29+0\\ 24+5 & 12+3\\ 32+70 & 16+42\\ 22+5 & 11+3\\ 24+155 & 12+93\end{pmatrix}=\begin{pmatrix}44 & 24\\ 66 & 37\\ 58 & 29\\ 29 & 15\\ 102 & 58\\ 27 & 14\\ 179 & 105\end{pmatrix}$$

Yuqoridagilaran shifrlangan matritsani sonlar qatoriga aylantirsak

44-24-66-37-58-29-29-15-102-58-27-14-179-105

Bu to‘la shifrlangan xabar. Endi uni o‘qish uchun shifr matritsa va yuqoridagi jadval kerak bo‘ladi. Shifrni ochish jarayoni quyidagicha bo‘ladi.

a). Berilgan shifr matritsa uchun teskari matritsa topiladi

$$A^{-1}=\begin{pmatrix}3 & -1\\ -5 & 2\end{pmatrix}$$

b). Shifrlangan matritsaga teskari matritsani ko‘paytiramiz

$$\begin{pmatrix} 44 & 24 \\ 66 & 37 \\ 58 & 29 \\ 29 & 15 \\ 102 & 58 \\ 27 & 14 \\ 179 & 105 \end{pmatrix} \cdot \begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix} = \begin{pmatrix} 12 & 4 \\ 13 & 8 \\ 29 & 0 \\ 12 & 1 \\ 16 & 14 \\ 11 & 1 \\ 12 & 31 \end{pmatrix}$$

d). Hosil bo‘lgan matritsadagi raqamlarni jadvaldagi harflarga aylantirib berilgan xabar olinadi.

Natijada, 12-4-13-8-29-0-12-1-16-14-11-1-12-31 ni yozib olamiz

Endi lotin alifbosidan foydalanib

A	B	D	E	F	G	H	I	J	K	L
1	2	3	4	5	6	7	8	9	10	11
M	N	O	P	Q	R	S	T	U	V	X
12	13	14	15	16	17	18	19	20	21	22
Y	Z	O‘	G‘	Sh	Ch	Ng	’	.		
23	24	25	26	27	28	29	30	31	0	

Izoh: 0 raqami bo‘sh joy(probel)ni mos qo‘yamiz.

Quyidagi xabar kelib chiqadi.

Xabar: Mening maqolam.

Adabiyotlar:

1. Курош А.Г. Курс высшей алгебры. 2008. – 432 с.

2. Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev, F.H.Haydarov Algebra va sonlar nazariyasi , Toshkent «Tafakkur-bo‘stoni» 2019 y.

3. Хожиев Ж.Х. Файнлейб А.С. Алгебра ва сонлар назарияси курси, Тошкент, «Ўзбекистон», 2001 й.

4. https://youtu.be/TJQD4dnCbAA

5. https://youtu.be/vrxzWNTtF68