7. N.Raximov, O.Primqulov, B.Daminova,“Basic concepts and stages of research development on artificial intelligence”, International Conference on Information Science and Communications Technologies (ICISCT), www.ieeexplore.ieee.org/document/9670085/metrics#metrics

8. N.Rahimov, D.Khasanov, “The mathematical essence of logistic regression for machine learning”, International Journal of Contemporary Scientific and Technical Research. Pg. 102-105.

9. Khasanov Dilmurod, Tojiyev Ma’ruf,Primqulov Oybek., “Gradient Descent In Machine”. International Conference on Information Science and Communications Technologies (ICISCT), https://ieeexplore.ieee.org/document/9670169

10. Babomurodov O. Zh., Rakhimov N. O. Stages of knowledge extraction from electronic information resources. Eurasian Union of Scientists. International Popular Science Bulletin. Issue. № 10(19)/2015. – pp. 130-133. ISSN: 2411-6467

11. N Raximov, M Doshchanova, O Primqulov, J Quvondikov. Development of architecture of intellectual information system supporting decision-making for health of sportsmen.// 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)Prasun Biswas, “Loss function in deep learning and python implementation”(web article), www.towardsdatascience.com, 2021.

12. Rahimov Nodir, Khasanov Dilmurod. (2022). The Mathematical Essence Of Logistic Regression For Machine Learning. https://doi.org/10.5281/zenodo.7239169

13. T. Maruf, "Hazard recognition system based on violation of the integrity of the field and changes in the intensity of illumination on the video image," 2022 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2022, pp. 1-3, doi: 10.1109/ICISCT55600.2022.10146933

14. Ma’ruf Tojiyev, Ravshan Shirinboyev, Jahongirjon Bobolov. Image Segmentation By Otsu Method. International Journal of Contemporary Scientific and Technical Research, (Special Issue), 2023. 64–72, https://zenodo.org/record/7630893

MULOHAZALAR VA MATRITSALARNING O‘ZORO BOG‘LANISHI

Maniyozov Oybek Azatboyevich
Toshkent axborot texnologiyalari univeristeti Farg‘ona filiali
maniyozovo@gmail.com

Annotatsiya: Ushbu maqolada mulohalar va matritsalar bog‘lanishi, mulohazalarni shifrlash, shirflangan ma’lumotlarni yechish, matritsalar ko’paytmasi hamda teskari matritsalarni Matlab programmasida ishlatish haqida ma’lumot berilgan.

Kalit so‘zlar: Mulohaza, sodda mulohaza, shifr matritsa, teskari matritsa, matritsalar ko‘paytmasi.

Insonlar kundalik hayotda o‘zaro muloqot qilish uchun turli mulohazalardan foydalanishadi. Ma’lumki, mulohaza – narsa yoki hodisalarning xususiyatini anglatuvchi darak gapdir. Boshqacha aytganda, mulohaza – rost yoki yolg‘onligi haqida so‘z yuritish mumkin bo‘lgan darak gap.

Mulohazalar sodda va murakkab bo‘lishi mumkin. Biror shart yoki usul bilan bog‘lanmagan hamda faqat bir holatni ifodalovchi mulohazalar sodda mulohazalar deyiladi. Sodda mulohazalar ustida amallar bajarib, murakkab mulohazalarni hosil qilish mumkin.

Shu mulohazalariz ya’ni muloqotlarimiz tegishli doirada dahlsiz yoki sir saqlanishi uchun matritsalardan foydalanamiz. Matritsalarni turli mazmundagi xabarlarni shifrlashda foydalanish mumkin. Buning uchun foydalaniladigan alifboni raqamlashtirib olishimiz kerak bo‘ladi.

Masalan: Lotin alifbosidagi harflarni raqamlashtirish jadvali. (1-jadval)

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**	**V**	**Z**	**·**			
21	22	23	24	25	26	27	0		

(0 raqamiga bo‘sh joy{probel}ni bosib qo‘yamiz).

Keyin esa maxsus faqat kvadrat matritsadan iborat bo‘lgan **shifr matritsa** ni tanlab olamiz.

Misol uchun bizning shifr matritsamiz $\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$ ko‘rinishida bo‘lsin, so‘ngra berilgan mulohazamizni ya’ni xabarimizni yuqorida berilgan jadval asosida matritsaga aylantiramiz.

Dastlab xabarni sonlar orqali yozib olamiz. Xabar: **Men Toshkentdaman.**

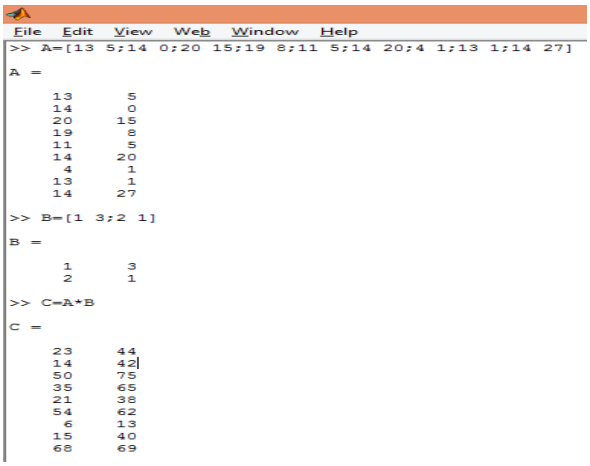
13-5-14-0-20-15-19-8-11-5-14-20-4-1-13-1-14-27

Endi esa bu sonlarni berilgan shifr matritsamizni ustunlar soniga mostlab ikki ustunli matritsa ko‘rinishida yozamiz. $\begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 15 \\ 19 & 8 \\ 11 & 5 \\ 14 & 20 \\ 4 & 1 \\ 13 & 1 \\ 14 & 27 \end{pmatrix}$.

Xosil bo‘lgan matritsamizni shifr matritsamizga ko‘paytirsak shirflangan muloxaza matritsasi xosil bo‘ladi[1]-[4]

$$\begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 15 \\ 19 & 8 \\ 11 & 5 \\ 14 & 20 \\ 4 & 1 \\ 13 & 1 \\ 14 & 27 \end{pmatrix} * \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 23 & 44 \\ 14 & 42 \\ 50 & 75 \\ 35 & 65 \\ 21 & 38 \\ 54 & 62 \\ 6 & 13 \\ 15 & 40 \\ 68 & 69 \end{pmatrix}.$$

Matritsalarni ko‘paytamsini MATLAB programmasi yordamida tekshirib qo‘yamiz. (1-rasm)



1-rasm. Matritsalarni Matlab programmasida ko‘paytmasi

Shifrlangan matritsamizni yana sonlar qatoriga aylantirib olsak
23-44-14-42-50-75-35-65-21-38-54-62-6-12-15-40-68-69

Bu biz yaratgan shirflangan muloxaza.

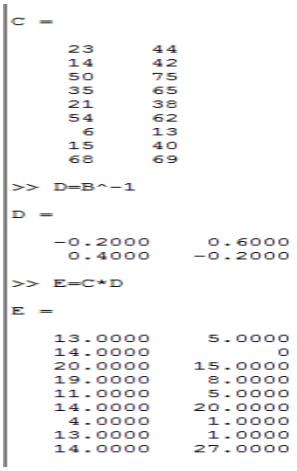
Shifrlangan muloxazani o‘qib olish uchun yuqorida keltirilgan jadval hamda shifr matritsamiz kerak bo‘ladi. Buning uchun dastalab shifr matritsamizni teskari matritsasini topib olamiz.

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

Keyin esa shifrlangan muloxaza matritsamizni teskari matritsaga ko‘paytiramiz[1;4].

$$\begin{pmatrix} 23 & 44 \\ 14 & 42 \\ 50 & 75 \\ 35 & 65 \\ 21 & 38 \\ 54 & 62 \\ 6 & 13 \\ 15 & 40 \\ 68 & 69 \end{pmatrix} * \begin{pmatrix} \frac{-1}{5} & \frac{3}{5} \\ \frac{2}{5} & \frac{-1}{5} \end{pmatrix} = \begin{pmatrix} 13 & 5 \\ 14 & 0 \\ 20 & 15 \\ 19 & 8 \\ 11 & 5 \\ 14 & 20 \\ 4 & 1 \\ 13 & 1 \\ 14 & 27 \end{pmatrix}$$

Yuqoridagi ko‘paytmani MATLAB da tekshirish. (2-rasm)



2-rasm. Matlabda shifrlangan muloxazani teskari shifr matritsaga ko‘paytirish

Xosil bo‘lgan matritsamizni jadval asosida harflarga aylantirsak dastlabki xabar olinadi.

Matritsalarni bir biriga ko‘paytiirsh, teskari matritsasini MATLAB dasturidan foydalanib olishingiz mumkin [5]

Xulosa qilib aytish mumkinki, xozirgi axborot texnologiyalari asrining muhim masalalarini Oliy matematikaning “Matritsalar va ular ustida amallar” bo’limi yordamida hal qilish mumkinlagini ko‘rsatamiz. Bu esa keng jamoatchilik o‘rtasida juda qiziqarli hamda ommalashishiga ishonamiz.

Foydalanilgan adabiyotlar ro‘yxati:

1. Rajabov F. Oliy matematika. O‘quv qo‘llanma(72), 2007-400b
2. Sh. Xurramov. “Oliy matematika”. 1-2 jild.(18) Toshkent,“Tafakkur” nashriyoti, 2018.-492b.
3. ManiyozovO.A, (2022). MATEMATIKA TA’LIMIDA RAQAMLI TEXNOLOGIYALARNING AFZALLIKLARI VA KAMCHILIKLARI. *Academic research in educational sciences*, *3*(10), 901-905.
4. T.Dadajonov, M.Muhiddinov “MATLAB asoslari” “Fan nashriyoti” 2008yil 34-37-bet
5. Xudayarov B.A. Matematika. Darslik. 1-qism: Chiziqli algebra va analitik geometriya. O’zR Oliy va o’rta maxsus ta’lim vazirligi.(10)2018.-284 bet
6. Nasriddinov, O., Maniyozov, O., & Bozorqulov, A. (2023). XUSUSIY HOSILALI DIFFERENSIAL TENGLAMALARNING UMUMIY YECHIMNI TOPISHNING XARAKTERISTIKALAR USULI. *Research and implementation*.
7. Minorskiy V.P. Oliy matematika masalalari to‘plami. Oliy o‘quv yurtlari uchun o‘quv qo‘llanma. (39).1977.-368b
8. Maniyozov, O., Bozorqulov, A., & Isomiddinova, O. (2023). TA’LIM JARAYONIDA BIRINCHI TARTIBLI CHIZIQLI ODDIY DIFFERENSIAL TENGLAMALARNING YECHIMINI MAPLE DASTURIDA TOPISH. *Farg‘ona davlat universiteti ilmiy jurnali*, (1), 190-202.

9. Tolipov, N., Xudoynazarov, Q., & Munavarjonov, S. (2023). ОБ ОДНОЙ НЕКОРРЕКТНОЙ ЗАДАЧЕ ДЛЯ БИГАРМОНИЧЕСКОГО УРАВНЕНИЯ В ПОЛУШАРЕ. *Research and implementation*.
10. To‘xtasinov, D. F., & qizi Abdullayeva, S. H. (2023). MATEMATIKA DARSLARIDA IJODIY TAFAKKURNI RIVOJLANTIRISH SHARTLARINING DIDAKTIK KOMPLEKSINI AMALIYOTDA QO‘LLASH YO‘LLARI. *Educational Research in Universal Sciences*, *2*(2), 613-616.

SM4 SHIFRLASH ALGORITMINI APPARAT AMALGA OSHIRISH USULLARI

Olimov Iskandar Salimboyevich,
Korabayev Eldor Alijonovich,
Karimov Abduqodir Abdusalomovich
Toshkent axborot texnologiyalari universiteti
karimovabduqodir041@gmail.com

Annotatsiya: Ushbu maqolada SM4 shifrlash algoritmini amalga oshirish usullariga bag‘ishlangan bo‘lib, unda SM4 shifrlash algoritmini ma’lumotlarni maxfiyligini ta’minlashdagi o‘rni, ishlash funksiyasi shu bilan birga aparat amalga oshirish usullari va ularni tahlili keltirilgan.

Kalit so‘zlar: SM4, feystel tarmog‘i, FPGA, Elektron Codebook (ECB), Cipher Block Chaining (CBC).

SMS4 nomi bilan ham tanilgan SM4 shifr 2007 yilda Xitoy Milliy Kriptografiya Byurosi tadqiqotchilari tomonidan ishlab chiqilgan. U Xitoy uchun ma’lumotlar maxfiyligini ta’minlashda foydanilgan shifrlash standarti DES va uning vorisi o‘rnini bosuvchi milliy standart shifrlash algoritmi sifatida ishlab chiqilgan.

SM4 shifrlash algoritmi feystel tarmog‘iga asoslangan bo‘lib, uni blok uzunligi 128 bitni tashkil etadi, bu 16 baytga teng. Bu shuni anglatadiki, SM4 shifrlash va shifrni ochish jarayonida bir vaqtning o'zida 128 bitli bloklarda foydaniladi [1,2].
Umumiy olganda 128 bitli blok o'lchami zamonaviy blok shifrlari uchun keng tarqalgan tanlovdir, chunki u xavfsizlik va samaradorlik o'rtasidagi muvozanatni ta'minlaydi. Blokning kattaroq o'lchami ko'proq mumkin bo'lgan kirishlar to'plamini joylashtirish orqali xavfsizlikni oshirishi mumkin, ammo u hisoblashning murakkabligini oshirishi va qayta ishlashni sekinlashtirishi mumkin.1-rasm. Feystel tarmog‘iga asoslangan SM4 shifrlash algoritmi.

Aksincha, kichikroq blok o'lchami samaraliroq bo'lishi mumkin, ammo kirish maydoni cheklanganligi sababli ma'lum turdagi hujumlarga moyil bo'lishi mumkin.

SMS4 algoritmi sifatida ham tanilgan SM4 shifrlash algoritmi ma'lumotlarni shifrlash va shifrini ochish uchun ishlatiladigan simmetrik blokli shifrdir. Bu Xitoyda keng tarqalgan bo'lib qabul qilingan standart bo'lib, turli ilovalarda, jumladan xavfsiz aloqa va ma'lumotlarni himoya qilishda qo'llaniladi. Bu maqolada SM4 algoritmining apparat amalga oshirish jihatlari haqida umumiy ma'lumot keltirilgan [2,3]: