7 – TOM 6 – SON / 2024 - YIL / 15 - IYUN

SIMMETRIK VA OCHIQ KALITLI (NOSIMMETRIK) KRIPTOTIZIMLAR

Sharopova Muxayyo Muxtor qizi
Osiyo Xalqaro Universiteti
"Umumtexnik fanlar" kafedrasi o'qituvchisi
muxayyosharopova4@gmail.com

Annotatsiya: *Ushbu maqolada kriptografik tizim, simmetrik kriptotizim va shifrlash turlari va xususiyatlari keltirib o'tilgan. Turli shiflash algoritmlari haqida ma'lumotlar berilgan*

Annotation: *In this article, the cryptographic system, symmetric cryptosystem and types and features of encryption are mentioned. Information about various healing algorithms is provided*

Kirish

Kriptografik tizim, yoki qisqacha, kriptotizim shifrlash ham shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shu kalitlarni boshqaruv tizimi hamda shifrlanadigan va shifrlangan matnlarning o'zaro bog'langan majmuasidir. Kriptotizimdan foydalanishda matn egasi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o'giradi. Matn egasi uni o'zi foydalanishi uchun shifrlagan bo'lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo'lmaydi) saqlab qo'yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asliga (dastlabki matn) aynan bo'lsa, saqlab qo'yilgan axborotning butunligiga ishonch hosil bo'ladi. Aks holda axborot butunligi buzilgan bo'lib chiqadi. Agar shifrlangan matn undan qonuniy foydalanuvchiga(oluvchiga) mo'ljallangan bo'lsa, u tegishli manzilga jo'natiladi. So'ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma'lum bo'lgan shifr ochish kaliti va algoritmi vositasida dastlabki matnga aylantiriladi. Bunda kalitni 9 qanday hosil qilish, aloqa qatnashchilariga bu kalitni maxfiyligi saqlangan holda yetkazish, va umuman, ishtirokchilar orasida kalit uzatilgunga qadar xavfsiz aloqa kanalini hosil qilish asosiy muammo bo'lib turadi. Undan tashqari yana boshqa bir muammo – autentifikatsiya muammosi ham ko'ndalang bo'ladi. Chunki, dastlabki matn(xabar) shifrlash kalitiga ega bo'lgan kimsa tomonidan shifrlanadi. Bu kimsa kalitning haqiqiy egasi bo'lishi ham, begona (mabodo kriptotizimning siri ochilgan bo'lsa) bo'lishi ham mumkin. Aloqa ishtirokchilari shifrlash kalitini olishganda u chindan ham shu kalitni yaratishga vakolatli kimsa tomonidan yoki tajovuzkor tomonidan yuborilgan bo'lishi ham mumkin. Bu muammolarni turli kriptotizimlar turlicha hal qilib beradi. Simmetrik kriptotizimda kalit aloqaning ikkala tomoni uchun bir xil maxfiy va ikkovlaridan boshqa hech kimga oshkor bo'lmasligi shart. Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog'liq. Simmetrik kriptotizimlar uzoq o'tmishga ega bo'lsa da, ular asosida olingan algoritmlar

kompyuterlardagi axborotlarni himoyalash zarurati tufayli ba'zi davlatlarda standart maqomiga ko'tarildilar. Masalan, AQShda ma'lumotlarni shifrlash standarti sifatida AES(Advanced Encryption Standart) algoritmi 2000 yilda qabul qilingan. Rossiyada unga o'xshash standart GOST 28147-89 sifatida 128 bitli kalit bilan ishlaydigan algoritm 1989 yilda tasdiqlangan. Bular dastlabki axborotni 64 bitli bloklarga bo'lib alohida yoki bir-biriga bog'liq holda shifrlashga asoslanganlar. Algoritmlarning matematikaviy asosida axborot bitlarini aralashtirish, o'rniga qo'yish, o'rin almashtirish va modul bo'yicha qo'shish amallari yotadi. Unda kirish va chiqishdagi matnlarning axborot miqdorlari deyarli bir xil bo'ladi. Bunday tizimning xavfsizligi asosan maxfiy kalitning himoya xossalariga bog'liq. Simmetrik kriptotizimdan foydalanib elektron yozishmalar boshlash uchun avvalo maxfiy kalitni yoki parolni ikki aloqa ishtirokchisidan biri ikkinchisiga maxfiy holda yetkazishi kerak. Maxfiy kalitni yetkazish uchun maxfiy aloqa kanali(shaxsan uchrashish, himoyalangan aloqa kanali va sh.o'.) kerak. Shunday qilib yopiq davra hosil bo'ladi: maxfiy kalitni topshirish uchun maxfiy kanal kerak, maxfiy kanalni hosil qilish uchun maxfiy kalit kerak. Maxfiy kalit tez-tez o'zgartirilib turilsa (aslida, har bir yozishmaga alohida maxfiy kalit ishlatilganda eng yuqori maxfiylikka erishiladi) bu muammo doimo ko'ndalang bo'laveradi. Shifrlash va shifr ochish kalitlari o'zaro funktsional bog'langan bo'lib ulardan biri asosida ikkinchisi amaliy jihatdan (mavjud hisoblash vositalari taraqqiyoti darajasida) hisoblab topilishi mumkin bo'lmagan va ulardan biri faqat bitta aloqa ishtirokchisiga ma'lum bo'lib boshqalardan 10 maxfiy tutiladigan, ikkinchisi esa aloqa ishtirokchilarining hammasiga oshkor bo'lgan kriptotizim nosimmetrik (sinonimlari: ochiq kalitli, ikki kalitli) kriptotizim deb ataladi. Nosimmetrik kriptotizim ikki kalitli tizim bo'lib, unda aloqa ishtirokchilarining har biri o'zining shaxsiy maxfiy va ochiq kalitlari juftiga ega bo'lib o'z ochiq kalitini boshqa aloqa ishtirokchilariga e'lon qiladi. Shaxsiy yopiq kalit qabul qilinadigan axborot pinhonligini ta'minlash uchun yaratilganda shifrni ochish kaliti bo'lib xizmat qiladi. Bunda kimga pinhona axborot jo'natiladigan bo'lsa shuning ochiq kalitidan foydalanib shifrlangan axborot jo'natiladi. Bunday axborotning shifrini faqat yagona yopiq kalit egasigina ocha oladi. Agar maxfiy kalit autentifikatsiya maqsadida jo'natmalarga raqamli imzo bosish uchun hosil qilingan bo'lsa, u shifrlash kaliti sifatida foydalaniladi. Ochiq kalit esa yuqoridagi birinchi holda shifrlash kaliti bo'lib, ikkinchi holda shifrni ochish (tekshirib ko'rish) kaliti bo'lib xizmat qiladi. Nosimmetrik kriptotizimlar asoslari simmetrik tizimlarda yechilmay qolgan kalit tarqatish va raqamli imzo muammolarining yechimini izlash yo'llarida Massachuset texnologiya institutida U.Diffi (W.Diffie) va uning ilmiy rahbari M.Xellman (M.E.Hellman) tomonidan 1975 yilda taklif etilgan. 1977 yili shu tamoyil asosida o'sha institutda R.Rivest, A.Shamir, L.Adlman (R.Rivest, A.Shamir, L.Adleman) tomonidan RSA algoritmi ishlab chiqildi. Keyinchalik elliptik va sh.o'. bir tomonlama oson hisoblanadigan funksiyalar asosiga qurilgan boshqa algoritmlar yaratildi. Nosimmetrik kriptotizimlar simmetrik kriptotizimlarga nisbatan o'nlab marta ko'proq axborot

miqdoriga ega (512, 1024, 2048, 4096 bitli) kalitlardan foydalanadi va shunga ko'ra yuzlab marta sekinroq ishlaydi. Nosimmetrik kriptotizimlarning matematik asosida bir tomonlama oson hisoblanadigan funksiyalar (darajaga oshirish, elliptik funksiya, rekursiya va sh.o'.) yotadi. Yashirin yo'lli birtomonlama funksiyalardan foydalanilganda

FOYDALANILGAN ADABIYOTLAR:

1. Sharopova, M. (2024). GAMMALASHTIRISHGA ASOSLANGAN SHIFRLASH ALGORITMLARINING MATEMATIK ASOSLARI. *Центральноазиатский журнал образования и инноваций*, *3*(2 Part 2), 113-115.

2. Sharopova, M. (2024). AES KRIPTOALGORITMINING MATEMATIK ASOSI. *Development of pedagogical technologies in modern sciences*, *3*(3), 188-192.

3. qizi Sharopova, M. M. (2023). RSA VA EL-GAMAL OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDA ELEKTRON RAQMLI IMZOLARI. RSA OCHIQ KALITLI SHIFRLASH ALGORITMI ASOSIDAGI ELEKTRON RAQAMLI IMZO. *Educational Research in Universal Sciences*, *2*(10), 316-319.

4. Sharopova, M. M. qizi . (2023). JAVA TILI YORDAMIDA OB'EKTGA YUNALTIRILGAN DASTURLASH ASOSLARI BILAN TANISHISH. GOLDEN BRAIN, 1(34), 111–119.

5. Sharopova, M. (2023). ARRAY AND ARRAYS INSTALLATION. *Development of pedagogical technologies in modern sciences*, *2*(12), 102-107.

6. qizi Sharopova, M. M. (2023). INTRODUCING" PROGRAM CONTROL OPERATORS" IN THE JAVA PROGRAMMING LANGUAGE. *Multidisciplinary Journal of Science and Technology*, *3*(5), 222-231.

7. qizi Sharopova, M. M. (2023). Working with folders in the JAVA programming language. *Multidisciplinary Journal of Science and Technology*, *3*(5), 232-236.

8. Sharopova, M. (2024). DSA ERI STANDARD. ELECTRONIC DIGITAL SIGNATURE OF GOST R 34.10-94. *Theoretical aspects in the formation of pedagogical sciences*, *3*(1), 169-178.

9. Sharopova, M. (2024). ELECTRONIC DIGITAL SIGNATURE ALGORITHMS BASED ON THE COMPLEXITY OF THE FACTORIZATION PROBLEM. *Science and innovation in the education system*, *3*(1), 66-74.Sharopova, M. (2024). BANK ISHIDA AXBOROT TEXNOLOGIYALARI FUNKTSIYALARI. KREDIT OPERATSIYALARINING AXBOROT TIZIMLARI. *PEDAGOG*, *7*(5), 270-276.

10. Sharopova, M. (2024). AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI. BIZNES BOSHQARUVIDA AVTOMATLASHTIRILGAN AXBOROT TIZIMLARI. *Multidisciplinary Journal of Science and Technology*, *4*(3), 781-789.

11. Sharopova, M. (2024). BANK ISHIDA AXBOROT TEXNOLOGIYALARI FUNKTSIYALARI. KREDIT OPERATSIYALARINING AXBOROT TIZIMLARI. *PEDAGOG*, *7*(5), 270-276.

12. Behruz Ulugbek og, Q. (2024). ADOBE PHOTOSHOP CC DASTURIDA ISHLASH. *PEDAGOG*, *7*(4), 390-396.

13. Behruz Ulugbek og, Q. (2024). FUNDAMENTALS OF ALGORITHM AND PROGRAMMING IN MATHCAD SOFTWARE. *Multidisciplinary Journal of Science and Technology*, *4*(3), 410-418.

14. Behruz Ulug'bek o'g, Q. (2023). USE OF ARTIFICIAL NERVOUS SYSTEMS IN MODELING. *Multidisciplinary Journal of Science and Technology*, *3*(5), 269-273.

15. Quvvatov, B. (2024). ALGEBRAIK ANIQLIGI YUQORI BOLGAN KVADRATUR FORMULALAR. KLASSIK GAUSS KVADRATURALARI. *Инновационные исследования в науке*, *3*(2), 94-103.

16. Quvvatov, B. (2024). ALGEBRAIK ANIQLIGI YUQORI BOLGAN KVADRATUR FORMULALAR. SIMPSON FORMULASI. *Models and methods in modern science*, *3*(2), 223-228.

17. Quvvatov, B. (2024). ALGEBRAIK ANIQLIGI YUQORI BOLGAN KVADRATUR FORMULALAR. ROMBERG INTEGRALLASH FORMULASI. *Центральноазиатский журнал образования и инноваций*, *3*(2 Part 2), 107-112.

18. Quvvatov, B. (2024, February). TORTBURCHAK ELEMENT USTIDA GAUSS–LEJANDR FORMULASI. In *Международная конференция академических наук* (Vol. 3, No. 2, pp. 101-108).

19. Boboqulova, M., & Sattorova, J. (2024). OPTIK QURILMALARDAN TIBBIYOTDA FOYDALANISH. B INNOVATIVE RESEARCH IN SCIENCE (T. 3, Выпуск 2, cc. 70–83).

20. Boboqulova, M. (2024). FIZIKAVIY QONUNIYATLARNI TIRIK ORGANIZMDAGI JARAYONLARGA TADBIQ ETISH . B MODELS AND METHODS IN MODERN SCIENCE (T. 3, Выпуск 2, cc. 174–187).

21. Boboqulova, M. (2024). IONLOVCHI NURLARNING DOZIMETRIYASI VA XOSSALARI. B DEVELOPMENT AND INNOVATIONS IN SCIENCE (T. 3, Выпуск 2, cc. 110–125).

22. Boboqulova, M. (2024). KVANT NAZARIYASINING TABIATDAGI TALQINI. B ACADEMIC RESEARCH IN MODERN SCIENCE (T. 3, Выпуск 7, cc. 68–81).

23. Muxtaram Boboqulova Xamroyevna. (2024). QUYOSH ENERGIYASIDAN FOYDALANISH . TADQIQOTLAR.UZ, 34(2), 213–220.

24. Xamroyevna, M. B. (2024). Klassik fizika rivojlanishida kvant fizikasining orni. Ta'limning zamonaviy transformatsiyasi, 6(1), 9-19.

25. Xamroyevna, M. B. (2024). ELEKTRON MIKROSKOPIYA USULLARINI TIBBIYOTDA AHAMIYATI. *PEDAGOG*, *7*(4), 273-280.

26. Boboqulova, M. X. (2024). FIZIKANING ISTIQBOLLI TADQIQOTLARI. *PEDAGOG*, *7*(5), 277-283.

27. Muxtaram Boboqulova Xamroyevna. (2024). GEYZENBERG NOANIQLIK PRINTSIPINING UMUMIY TUZILISHI . TADQIQOTLAR.UZ, 34(3), 3–12.

28. Muxtaram Boboqulova Xamroyevna. (2024). THERMODYNAMICS OF LIVING SYSTEMS. Multidisciplinary Journal of Science and Technology, 4(3), 303–308.

29. Sharipova, M. (2024). IKKI NOMALUMLI TENGLAMANING GEOMETRIK MANOSI. *Бюллетень педагогов нового Узбекистана*, *2*(2), 41-51.

30. Sharipova, M. (2024). BIRINCHI DARAJALI TAQQOSLAMALAR SISTEMALARI. *Центральноазиатский журнал академических исследований*, *2*(2), 11-22.

31. Sharipova, M., & Latipova, S. (2024). TAQQOSLAMALAR. EYLER FUNKSIYASI. *Бюллетень студентов нового Узбекистана*, *2*(2), 23-33.

32. Sharipova, M., & Latipova, S. (2024). IKKI O'ZGARUVCHILI TENGLAMALAR SISTEMASI. *Центральноазиатский журнал образования и инноваций*, *3*(2 Part 2), 93-103.

33. Po'latovna, S. M. (2024). ANIQ INTEGRALLARNI TAQRIBIY HISOBLASH. *PEDAGOG*, *7*(4), 158-165.

34. Sharipova, M. P. L. (2024). I TARTIBLI DIFFERENSIAL TENGLAMALARNING AYRIM IQTISODIY TATBIQLARI. *PEDAGOG*, *7*(5), 610-617.

35. Latipova, S. (2024). BIRINCHI TARTIBLI HOSILA YORDAMIDA FUNKSIYANING EKSTREMUMGA TEKSHIRISH, FUNKSIYANING EKSTREMUMLARI. B CENTRAL ASIAN JOURNAL OF EDUCATION AND INNOVATION (Т. 3, Выпуск 2, сс. 66–72).

36. Sharipova, M., & Latipova, S. (2024). TAKRORIY GRUPPALASHLAR. *Development of pedagogical technologies in modern sciences*, *3*(3), 134-142.

37. Shahnoza Latipova. (2024). THE STRAIGHT LINE AND ITS DIFFERENT DEFINITIONS. Multidisciplinary Journal of Science and Technology, 4(3), 771–780.

38. Latipova, S. (2024). KO ‘PO ‘ZGARUVCHILI FUNKSIYALARNING TURLI TA’RIFLARI. *PEDAGOG*, *7*(5), 618-626.

39. Ikromovna, A. Z. (2024). TEST TIZIMDA AVTOMATLASHTIRILGAN DASTURINI YARATISH. *PEDAGOG*, *7*(5), 259-269.

40. Axmedova, Z. (2024). KOMPYUTER TESTINING MAQSADI, MAZMUNI VA TUZILISHINI ANIQLASH. *Development of pedagogical technologies in modern sciences*, *3*(3), 201-206.

41. Axmedova, Z. (2024). TEST TIZMDA AVTOMATLASHTIRILGAN DASTURNI YARATISH BOSQICHLARI. *Центральноазиатский журнал академических исследований*, *2*(2), 23-32.

42. Axmedova, Z. (2024, February). MOBIL ILOVA YARATISHNI VIRTUAL O‘RGATISHDA GLOBAL AXBOROT TIZIMLARI VA TEXNOLOGIYALARI. In *Международная конференция академических наук* (Vol. 3, No. 2, pp. 71-84).

43. Akhmedova, Z. (2024). ORGANIZING THE EDUCATIONAL PROCESS IN THE EDUCATIONAL MANAGEMENT SYSTEM. *Models and methods in modern science*, *3*(1), 194-200.

44. Axmedova, Z. (2023). KOMPYUTERLASHTIRILGAN TESTLARNING XUSUSIYATLARI. *Theoretical aspects in the formation of pedagogical sciences*, *3*(4), 46-59.

45. Ashurov, J. D. (2024). TA'LIM JARAYONIDA SUN'IY INTELEKTNI QO'LLASHNING AHAMIYATI. PEDAGOG, 7(5), 698-704.

46. Djorayevich, A. J. (2022). EXPLANATION OF THE TOPIC" USE OF RADIOPHARMACEUTICALS IN GAMMA THERAPY" IN HIGHER EDUCATION INSTITUTIONS USING THE" THOUGHT, REASON, EXAMPLE, GENERALIZATION (THREG)" METHOD.

47. Djo‘rayevich, A. J. (2024). THE IMPORTANCE OF USING THE PEDAGOGICAL METHOD OF THE" INSERT" STRATEGY IN INFORMATION TECHNOLOGY PRACTICAL EXERCISES. Multidisciplinary Journal of Science and Technology, 4(3), 425-432.

48. Ashurov, J. (2023). TA’LIMDA AXBOROT TEXNOLOGIYALARI FANI O ‘QITISHDA INNOVATSION TA’LIM TEXNOLOGIYALARINING AHAMIYATI. Theoretical aspects in the formation of pedagogical sciences, 3(4), 105-109.

49. Ashurov, J. D. (2024). AXBOROT TEXNOLOGIYALARI VA JARAYONLARNI MATEMATIK MODELLASHTIRISH FANINI O ‘QITISHDA INNOVATSION YONDASHUVGA ASOSLANGAN METODLARNING AHAMIYATI. Zamonaviy fan va ta'lim yangiliklari xalqaro ilmiy jurnal, 2(1), 72-78.

50. Djuraevich, A. J. (2021). Zamonaviy ta'lim muhitida raqamli pedagogikaning o'rni va ahamiyati. Евразийский журнал академических исследований, 1(9), 103-107.
51. Djurayevich, A. J. (2021). Education and pedagogy. Journal of Pedagogical Inventions and Practices, 3, 179-180.
52. Ashurov, J. D. R. (2023). OLIY O 'QUV YURTLARI TALABALARIGA YADRO TIBBIYOTINI O 'QITISHDA INNOVATSION TA'LIM TEXNOLOGIYALAR VA METODLARINI QO 'LLASHNING AHAMIYATI. Results of National Scientific Research International Journal, 2(6), 137-144.
53. Ashurov, J. (2023). OLIY TA'LIM MUASSASALARIDA "RADIOFARMATSEVTIK PREPARATLARNING GAMMA TERAPIYADA QO 'LLANILISHI" MAVZUSINI "FIKR, SABAB, MISOL, UMUMLASHTIRISH (FSMU)" METODI YORDAMIDA YORITISH. Центральноазиатский журнал образования и инноваций, 2(6 Part 4), 175-181.
54. Ashurov, J. (2023). THE IMPORTANCE OF USING INNOVATIVE EDUCATIONAL TECHNOLOGIES IN TEACHING THE SCIENCE OF INFORMATION TECHNOLOGY AND MATHEMATICAL MODELING OF PROCESSES. Development and innovations in science, 2(12), 80-86.
55. Ashurov, J. (2023). KREDIT MODUL TIZIMIDA JORIY QILISHDA O 'QITUVCHI VA TALABALARNING HAMKORLIKDA ISHLASHINING AHAMIYATI. Бюллетень педагогов нового Узбекистана, 1(6 Part 2), 42-47.
56. Ashurov, J. D. (2023). THE IMPORTANCE OF ORGANIZING THE COOPERATION BETWEEN TEACHER AND THE STUDENTS IN THE CREDIT-MODULE TRAINING SYSTEM. Modern Scientific Research International Scientific Journal, 1(4), 16-24.
57. Ashurov, J. D. (2023). FSMU METODI YORDAMIDA "AXBOROT JARAYONLARINING DASTURIY TA 'MINOTI" MAVZUSINI YORITISH. Journal of new century innovations, 41(2), 238-243.
58. Djurayevich, A. J. (2021). Opportunities Of Digital Pedagogy in A Modern Educational Environment. Journal of Pedagogical Inventions and Practices, 3, 103-106.
59. To'raqulovich, M. O. (2024). OLIY TA'LIM MUASSASALARIDA TA'LIMNING INNOVASION TEXNOLOGIYALARDAN FOYDALANISH. *PEDAGOG*, 7(5), 627-635.
60. Murodov Oybek Turakulovich. (2024). Development of an automated system for controlling temperature and humidity in production rooms. Multidisciplinary Journal of Science and Technology, 4(3), 403–409.
61. Jalolov, T. S. (2024). ANALYSIS OF PSYCHOLOGICAL DATA USING SPSS PROGRAM. Multidisciplinary Journal of Science and Technology, 4(4), 477-482.

62. Jalolov, T. S. (2024). ИЗУЧЕНИЕ МАТЕМАТИЧЕСКИХ БИБЛИОТЕК PYTHON: ПОДРОБНОЕ РУКОВОДСТВО. MASTERS, 2(5), 48-54.
63. Jalolov, T. S. (2024). ВАЖНОСТЬ АНГЛИЙСКОГО ЯЗЫКА В ПРОГРАММИРОВАНИИ. MASTERS, 2(5), 55-61.