ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 9

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 9

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

O‘ZGARTIRISH, ALMASHTIRISH SP TARMOG‘IGA ASOSLANGAN SHIFRLASH ALGORITMLARI TAHLILI

Abdurazzoqov Javohir Rustamovich
Toshkent xalqaro universiteti “Aniq fanlar va raqamli texnologiyalar” kafedrasi dotsenti, E-mail: javohirjon.1992@gmail.com
ORCID: 0000-0002-8052-0078

Anostatsiya. Mazkur maqolada o‘zgartirish va almashtirish tamoyillariga asoslangan SP (Substitution–Permutation) tarmog‘ining blokli shifrlash algoritmlaridagi o‘rni tahlil qilingan. Tadqiqotda substitutsiya, permutatsiya va XOR amallari orqali ma’lumotlarni himoyalash jarayonlari yoritilgan. Shuningdek, AES hamda O‘z DSt 1105:2009 algoritmlarining matematik asoslari va ishlash prinsiplari ko‘rib chiqilgan. AES algoritmida GF(2^8) chekli maydoni ustidagi amallar, O‘z DSt 1105:2009 algoritmida esa diamatrisalar algebrasi asosida shifrlash jarayoni amalga oshirilishi tahlil etilgan. Natijada SP tarmog‘iga asoslangan algoritmlar yuqori kriptografik bardoshlilik va axborot xavfsizligini ta’minlashda samarali ekani asoslab berilgan.

Kalit so‘zlar. SP tarmog‘i, blokli shifrlash, kriptografiya, substitutsiya, permutatsiya, XOR amali, AES, O‘z DSt 1105:2009, GF(2^8) maydoni, kriptobardoshlilik, axborot xavfsizligi, simmetrik shifrlash, raund funksiyasi, diamatrisa algebrai, shifrlash algoritmi.

Аннотация. В данной статье анализируется роль сети SP (Substitution–Permutation) в алгоритмах блочного шифрования, основанных на принципах замены и подстановки. Исследование охватывает процессы защиты данных посредством операций замены, перестановки и XOR. Также рассматриваются математические основы и принципы работы алгоритмов AES и Uz DSt 1105:2009. В алгоритме AES анализируются операции над конечным полем GF(28), а в алгоритме Uz DSt 1105:2009 процесс шифрования реализуется на основе алгебры диаматричек. В результате обосновывается эффективность алгоритмов, основанных на сети SP, в обеспечении высокой криптографической стойкости и информационной безопасности.

Ключевые слова: Сеть SP, блочный шифр, криптография, подстановка, перестановка, операция XOR, AES, Уз ДСт 1105:2009, поле GF(28), криптоустойчивость, информационная безопасность, симметричное шифрование, раундовая функция, алгебра диматричных матриц, алгоритм шифрования.

Abstract. This article analyzes the role of the SP (Substitution–Permutation) network in block encryption algorithms based on the principles of substitution and replacement. The study covers the processes of data protection through

substitution, permutation and XOR operations. Also, the mathematical foundations and principles of operation of the AES and Uz DSt 1105:2009 algorithms are considered. In the AES algorithm, operations on the finite field GF(28) are analyzed, and in the Uz DSt 1105:2009 algorithm, the encryption process is implemented based on the algebra of diamatrices. As a result, it is substantiated that algorithms based on the SP network are effective in ensuring high cryptographic strength and information security.

Keywords: SP network, block cipher, cryptography, substitution, permutation, XOR operation, AES, Uz DSt 1105:2009, GF(28) field, cryptoresistance, information security, symmetric encryption, round function, diamatrix algebra, encryption algorithm.

KIRISH.

Hozirgi kunda axborot almashinuvi hajmining ortishi va raqamli texnologiyalarning keng rivojlanishi ma’lumotlarni ishonchli himoyalash zaruratini kuchaytirmoqda. Shu sababli kriptografik himoya usullari axborot xavfsizligini таъминlashning muhim vositalaridan biri hisoblanadi. Ayniqsa, blokli shifrlash algoritmlari ma’lumotlarni xavfsiz uzatish va saqlashda keng qo‘llanilmoqda.

Zamonaviy blokli shifrlash algoritmlarining aksariyati SP (Substitution–Permutation) tarmog‘i asosida quriladi. Ushbu usulda ma’lumotlar substitutsiya va permutatsiya amallari orqali bir necha bosqichda qayta ishlanadi. Natijada shifrlangan ma’lumotning ochiq matn bilan bog‘liqligi kamayadi va algoritmning kriptografik bardoshliligi ortadi. Bugungi kunda AES algoritmi xalqaro standart sifatida keng foydalaniladi. Shuningdek, O‘z DSt 1105:2009 algoritmi ham ma’lumotlarni himoyalashda qo‘llaniladigan milliy blokli shifrlash standartlaridan biri hisoblanadi. Ushbu maqolada SP tarmog‘iga asoslangan shifrlash algoritmlarining ishlash prinsiplari, matematik asoslari va kriptografik xususiyatlari tahlil qilinadi.

METODOLOGIYA. Mazkur tadqiqotda SP (Substitution–Permutation) tarmog‘iga asoslangan blokli shifrlash algoritmlarining ishlash prinsipi va kriptografik xususiyatlarini tahlil qilish usullaridan foydalanildi. Tadqiqot obyekti sifatida AES hamda O‘z DSt 1105:2009 algoritmlari tanlandi.

Tadqiqot jarayonida algoritmlarning substitutsiya, permutatsiya va XOR amallariga asoslangan raundli tuzilishi o‘rganildi. AES algoritmida GF(2^8) chekli maydonidagi matematik amallar, S-box va MixColumns akslantirishlari tahlil qilindi. O‘z DSt 1105:2009 algoritmida esa diamatrisalar algebrasi, seans kalitlarini shakllantirish va bosqichli akslantirish jarayonlari ko‘rib chiqildi. Shuningdek, algoritmlarning kriptografik bardoshliligini baholashda qiyosiy tahlil usuli qo‘llanildi. Bunda kalit uzunligi, raundlar soni, ma’lumotlarni

ISSN 3030-3907

aralashtirish darajasi hamda kriptotahlilga chidamlilik ko‘rsatkichlari o‘zaro solishtirildi. Tadqiqot davomida nazariy tahlil, matematik modellashtirish va ilmiy manbalarni qiyosiy o‘rganish usullaridan foydalanildi.SPN (Substitution-Permutation Network) tarmoqining asoslangan shifrlash algoritmlari ham blokli shifrlashning mashhur va ommalashtirilgan usullaridan biridir. SPN, murojaatlar va tartiblangan murojaatlar (permutations) bilan o‘tkaziladi, shuningdek, murojaatlar uchun birinchi qism va ikkinchi qism arasida o‘zgarishlar (substitutions) qilinadi.

SPN tarmoqining amaliyoti quyidagi bosqichlardan iborat:

Kirish blokini almashish: Kirish blokining o‘lchamiga ko‘ra uning o‘lchamini kamaytirish yoki kattalashtirish mumkinligi bor.

Substitutsiya (Substitution): Kirish bloki ustida murojaatlar o‘zgarishlar (substitutions) amalga oshiriladi. Bu qadamda, kirish blokining har bir qismini belgilangan o‘zgaruvchanlar (substitution box) orqali o‘zgartiriladi.

Permutatsiya (Permutation): Substitutsiyadan so‘ng, o‘zgarishlar o‘tkaziladi va tartiblangan bloklar hosil qilinadi.

Raqam (Round): Yukoridagi bosqichlar bir necha marta takrorlanadi. Har takrorlash turishi uchun xususiy murojaat va permutatsiya funksiyalari ishlatiladi.

Yig‘indishtirish (XOR): Muhim qo‘llanma - ma’lumotlarni XOR (yoki boshqa bit bilan), kalitlar va murojaatlar orasida biriktirish. Bu xorlashlar ma’lumotlarni qo‘llab-quvvatlash uchun kritikdir.

Chiqish blokini almashish: Chiqish bloklari kirish bloklari bilan almashtirilishi mumkin.

SPN tarmoqining eng mashhur misollaridan biri AES (Advanced Encryption Standard) shifrlash algoritmi. AES, 128-bitlik kirish bloklarini 128-bitlik kalitlar bilan ishlatadi va murojaat va permutatsiya funksiyalarini amalga oshirish uchun belgilangan standartlarni qo‘llaydi.

SPN tarmoqining afzalliklari ichida yuqori xavfsizlik darajasi, yomon amaliyoti ta’siriga qarshi toza bo‘lishi, va platformalarda keng qo‘llanilishi kiritiladi. Ularning katta qismi, o‘zlarining blokli shifrlash usullari bo‘lib, axborotni himoya qilishda keng ishlatiladi.

NATIJALAR. Feystel tarmog‘iga asoslanmagan simmetrik blokli shifrlash algoritmlariga: AQSh davlat standarti **AES FIPS-197**, O‘zbekiston milliy standarti **O‘z DSt 1105:2009** simmetrik blokli shifrlash algoritmlari misol bo‘la oladi.

Quyida Feystel tarmog‘iga asoslanmagan simmetrik blokli shifrlash algoritmlari matematik asoslarini va keltirilgan algoritmlar akslantirishlari asosida yoritiladi.

ISSN 3030-3907

Amerika qo‘shma shtatlarining “Standartlar va texnologiyalar Milliy Instituti (NIST)” tomonidan 1997 yilda XXI asrning ma’lumotlarni kriptografik muhofazalovchi yangi shifrlash algoritmi standartini qabul qilish maqsadida tanlov e‘lon qilindi. 2000 yilda standart shifrlash algoritmi qilib RIJNDAEL shifrlash algoritmi asos qilib olingan AES (Advanced Encryption Standard) (FIPS 197) qabul qilindi. Algoritmning yaratuvchilari Belgiyalik mutaxassislar Yon Demen (Joan Daemen) va Vinsent Ryumen (Vincent Rijmen)larning familiyalaridan
RIJNDAEL nomi olingan.

AES FIPS-197 blokli shifrlash algoritmida 8 va 32-bitli (1-baytli va 4-baytli) vektorlar ustida amallar bajariladi. AES FIPS 197 shifrlash algoritmi XXI asrning eng barqaror shifrlash algoritmi deb hisoblanadi. Bu algoritm boshqa mavjud standart simmetrik shifrlash algoritmlaridan farqli o‘laroq, Feystel tarmog‘iga asoslanmagan blokli shifrlash algoritmlari qatoriga kiradi.

AES kriptoalgoritmining matematik asosi

AES algoritmida baytlar ustida amallar bajariladi. Baytlar $GF(2^8)$ chekli maydon elementlari sifatida qaraladi. $GF(2^8)$ maydon elementlarining darajasi 7 dan katta bo‘lmagan ko‘phad sifatida tasvirlash mumkin. Agarda baytlar

$$\{a_7a_6a_5a_4a_3a_2a_1a_0\}, a_i \in \{0,1\}, i = \overline{0 \dots 7},$$

ko‘rinishda tasvirlangan bo‘lsa, u holda maydon elementlari quyidagicha ko‘phad ko‘rinishda yoziladi:

$$a_7 \cdot x^7 + a_6 \cdot x^6 + a_5 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0.$$

Misol uchun $\{11010101\}$ baytga $x^7 + x^6 + x^4 + x^2 + a_0$ ko‘rinishdagi ko‘phad mos keladi.

Chekli $GF(2^8)$ maydon elementlari uchun additivlik va multiplikativlik xossalariga ega bo‘lgan qo‘shish va ko‘paytirish amallari aniqlangan.

Ko‘phadlarni qo‘shish

AES algoritmida ko‘phadlarni qo‘shish $\oplus$ **(XOR)** (berilgan ko‘phadlarga mos keluvchi ikkilik sanoq tizimidagi sonlarning mos bitlarini mod 2 bo‘yicha qo‘shish) amali orqali bajariladi. Masalan, $x^7 + x^6 + x^4 + x^2 + x$ va $x^7 + x^5 + x^3 + x + 1$ ko‘phadlar natijasi quyidagicha hisoblanadi:

$$(x^7 + x^6 + x^4 + x^2 + x) \oplus (x^7 + x^5 + x^3 + x + 1)$$
$$= (x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

Bu amal ikkilik va o‘n oltilik sanoq sistemalarida quyidagicha ifodalanadi:

$\{11010110\}_2 \oplus \{10101011\}_2 = \{01111101\}_2$ va $D6_{16} \oplus AB_{16} = 7D_{16}$.

Chekli maydonda istalgan nolga teng bo‘lmagan a element uchun unga teskari bo‘lgan $-a$ element mavjud va $a + (-a) = 0$ tenglik o‘rinli, bu yerda nol elementi sifatida $\{00\}_{16}$ qaraladi. $GF(2^8)$ maydonda $a \oplus a = 0$ tenglik o‘rinli.

ISSN 3030-3907

Ko‘phadlarni ko‘paytirish

AES algoritmida ko‘phadlarni ko‘paytirish quyidagicha amalga oshiriladi:

- ikkita ko‘phad o‘nlik sanoq tizimida ko‘paytiriladi;

- yettinchi darajadan katta bo‘lgan har qanday ko‘phadni sakkizinchi darajali $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ keltirilmaydigan ko‘phadga bo‘lganda qoldiqda yetti va undan kichik bo‘lgan darajadagi ko‘phadlar hosil bo‘lib, ular natija sifatida olinadi, bunda bo‘lish jarayonida bajariladigan ayirish amali ikkilik sanoq tizimida, yuqorida keltirilgani kabi, $\oplus$ amali asosida bajariladi.

AES FIPS-197 algoritmi raundlarining shifrlash jarayonlari:

SubBytes –berilgan jadval asosida baytlarni almashtirish, *ShiftRows* – berilgan jadval asosida baytlarni siklik surish, *MixColumns* –teskarisi mavjud bo‘lgan berilgan matrisa bo‘yicha baytlarni aralashtirish, AddRoundKey –raund kalitlari bloki bitlariga mos bloklar bitlarini XOR amali bilan qo‘shish akslantirishlarida iborat bo‘lib, bu akslantirishlarning bittasi, ya’ni AddRoundKey akslantirishi bir tomonlama hisoblanadi. Chunki raund kaliti bloki va unga XOR amali bilan qo‘shiluvchi mos blok noma’lum bo‘lib, bu akslantirish natijasi ma’lum bo‘lganda unga mos keluvchi blokni aniqlash uchun raund kalitini topish kerak bo‘ladi. Bunday holat esa raund kalitlarining barcha mumkin bo‘lgan qiymatlarini tanlab chiqishni talab etadi. Raund kalit uzunligining qanchalik katta bo‘lishi va raundlar sonining ko‘p bo‘lishi algoritm kriptobardoshliligini ifodalaydi. ***AES FIPS-197*** algoritmi raund kalitining eng kichik uzunligi 128 bit bo‘lib, barcha mumkin bo‘lgan qiymatlari soni 2^{128} ta, bu uzunlikdagi barcha mumkin bo‘lgan holatlarni tanlab chiqishni bugungi hisoblash texnika va texnologiyalari imkoniyatlaridan samarali foydalanilganda ham mumkin qadar qisqa vaqt ichida amalga oshirish ilojisi mavjud emas. Algoritm 10 raunddan iborat.

MUHOKAMA. O‘z DSt 1105:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi» standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi. Ma’lumotlarni shifrlash algoritmi (MShA) - simmetrik blokli shifr bo‘lib, axborotni shifrmatnga o‘girish va dastlabki matnga o‘girish uchun foydalaniladi. MShA *256* bit uzunlikdagi ma’lumotlar blokini shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girish uchun *256* yoki *512* bit uzunlikdagi kriptografik kalitdan foydalanishi mumkin.

O‘z DSt 1105:2009 kriptoalgoritmining matematik asosi

MShAda modul arifmetikasining diamatrisalar algebrasidan foydalaniladi, bunda hisoblashning qiyinlik darajasi matrisalar algebrasidagi singari bajariladi.

Shifrmatnga o‘girish va dastlabki matnga o‘girish proseduralarida foydalaniladigan diamatrisalar algebrasining asosiy amali diamatrisani p modul

ISSN 3030-3907

bo‘yicha diamatrisaga teskarilash amali hisoblanadi. Bu amallarda ikki o‘lchamli seans kaliti massivining maxsus tuzilmali 4x4 tartibli kvadrat diamatrisa bilan aks ettiriluvchi qismlari ishtirok etadi; maxsus tuzilmali diamatrisa uchun barcha diagonal elementlar bir xilligi, 1-satrdagi nodiagonal elementlar, shuningdek 2-satrning boshi va oxiridagi elementlar ham bir xilligi xosdir.

Maxsus tuzilmali diamatrisaning muhim xossasi diamatrisaning diaaniqlovchisini hisoblash formulasining soddaligidir, bu esa diamatrisani teskarilash shartlarini tekshirish ishlarini soddalashtiradi. Maxsus tuzilmali diamatrisaga nisbatan teskari diamatrisa o‘zining dastlabki tuzilmasini saqlaydi.

4x4 tartibli maxsus tuzilmali diamatrisa 10 ta har xil elementlar $a_0, \ldots, a_9$ dan tuzilgan bo‘lib, uning diaaniqlovchisi diagonal element a_7 ni uchta yig‘indiga ko‘paytmasi sifatida topiladi, bu yig‘indilardan har biri diagonal element bilan bitta satrda joylashgan unga o‘ngdan qo‘shni element bilan ustun elementlarining yig‘indisini ifodalaydi.

Maxsus diamatrisa uchun diaaniqlovchi a quyidagicha topiladi:

$$d \equiv a_7 x(a_7 + a_0 + a_8 + a_3 + a_5)x(a_7 + a_1 + a_8 + a_9 + a_6)x(a_7 + a_2 + a_8 + a_9 + a_4)(mod\ p).$$

Maxsus tuzilmali diamatrisani teskarilash shartlarini tekshirish MShA parametrlariga qo‘yiladigan asosiy talab hisoblanadi. U diagonal elementning qiymatlarini va aytib o‘tilgan ko‘paytmalarni 2 moduli bo‘yicha nol bilan taqqoslashga keltiriladi. Bu har qanday shifrlash kaliti va funksional kalitdan teskari diamatrisani shakllantirishga imkon beradi.

MShAda, shuningdek butun sonlarni parametrli ko‘paytirish, teskarilash va darajaga oshirish deb atalgan parametrli gruppa amallaridan ham foydalaniladi.

MShA uchun bosqich (raund)lar soni *ye=8* qilib belgilangan.

Ma’lumotlarni shifrlash algoritmining parametrlari va funksiyalari

MShA quyidagi parametr va funksiyalardan foydalanadi:

a) k – 256 yoki 512 bit uzunlikdagi shifrlash kaliti;

b) k_f – 256 bit uzunlikdagi funksional kalit;

c) K_{ye} – 8x4 (yoki 4x8) tartibli ikki o‘lchamli massiv shaklidagi bosqich kaliti;

d) b – 256 bit li kirish bloklari soni;

e) ye – bosqichlar soni, ye=8;

f) r, (r +1) – modul, r=256;

g) Aralash() – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirish uchun diamatrisaviy qismlar ustida amalga oshiriladi; mazkur shifralmashtirish kirishi Holat massivining diamatrisaviy qismlari hamda K_1 va K_2 massivlari bo‘lib, chiqishi Holat massividir;

h) BaytAlmash() – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda Holat massivi elementlarini almashtirish

ISSN 3030-3907

massivi elementlari bilan bayt sathida almashtirish uchun foydalaniladi; mazkur shifralmashtirish kirishi bayt sathida Holat massivi, almashtirish massivi chiziqli massiv B_{sA} [256] yoki B_{sAD} [256] bo‘lib, chiqishi bayt sathida Holat massividir;

i) Sur() – Holat massivi elementlarini yanada yaxshiroq aralashtirish uchun dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda foydalaniladi; mazkur almashtirish kirishi bayt sathida Holat massivi, chiqishi ustun bo‘ylab shifrlashda pastga va satr bo‘ylab o‘ngga yoki shifrni ochishda ustun bo‘ylab yuqoriga va satr bo‘ylab chapga surilgan bayt sathida Holat massividir;

j)ShaklSeansKalitBayt() – seans uchun kalit shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda BaytAlmash() shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi shifrlash kaliti k va funksional kalit k_f bo‘lib, chiqishi bayt sathida chiziqli massivlar B_{sA} [256] va B_{sAD} [256];

k) ShaklSeansKalit() – seans uchun kalitni shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda Aralash() shifralmashtirishni bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi baytli elementlardan tarkib topgan chiziqli massiv K_{st}=[32] bo‘lib, chiqishi maxsus tuzilmali diamatrisalardan tashkil topgan (K_{1t} , K_2) yoki (K_1 , K_{2t}) massivlar juftliklaridir;

l) ShaklBosqichKalit() – seans davomida seans-bosqich kalitidan bosqich kalitini shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda Qo‘shBosqichKalit() almashtirishini bajarish uchun foydalaniladi; mazkur almashtirish kirishi chiziqli seans-bosqich kaliti massivi k_{se}, chiqishi bayt sathida berilgan ikki o‘lchamli K_e[8,4] massividir;

m) Qo‘shBosqichKalit() – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda Holat va bosqich kaliti massivi K_e elementlari ustida istisnoli Yoki (2 moduli bo‘yicha bitlab qo‘shish) amalini bajarishdan iborat; mazkur shifralmashtirish kirishi bayt sathida Holat massivi, K_e massivi bo‘lib, chiqishi bayt sathida Holat massividir;

n) Qo‘shHolat() – oddiy shifralmashtirish bo‘lib, shifrlash bloklari ustida amalga oshiriladigan elektron kod kitobi rejimidan boshqa rejimlarda dastlabki matnni shifrmatnga va teskari yo‘nalishda XOR amali ishtirokida foydalaniladigan almashtirish.

MShA belgilab qo‘yilgan ikki xil - 256 va 512 bit uzunlikdagi kalitlar yordamida amalga oshiriladi.

XULOSA. Mazkur tadqiqotda SP (Substitution–Permutation) tarmog‘iga asoslangan blokli shifrlash algoritmlarining ishlash prinsiplari va matematik asoslari tahlil qilindi. Tadqiqot natijasida substitutsiya, permutatsiya hamda XOR amallari orqali ma’lumotlarni murakkab ko‘rinishga keltirish kriptografik

ISSN 3030-3907

bardoshlilikni oshirishi aniqlandi. Tahlillar asosida AES algoritmi GF(2^8) chekli maydoni ustidagi amallarga tayangan holda yuqori xavfsizlik va tezkorlikni ta'minlashi ko'rsatildi. Shuningdek, O'z DSt 1105:2009 algoritmida diamatrisalar algebrasi asosida amalga oshiriladigan akslantirishlar ma'lumotlarni himoyalash samaradorligini oshirishi tahlil qilindi.

Olib borilgan qiyosiy tahlillar SP tarmog'iga asoslangan blokli shifrlash algoritmlari zamonaviy axborot xavfsizligi tizimlarida samarali qo'llanilishini va ularning kriptotahlil usullariga nisbatan bardoshli ekanligini ko'rsatdi.Yuqorida ko'rib o'tilgan birinchi va ikkinchi holatlarda joriy seans uchun yangilangan funksional kalit k_f bundan oldingi seansda foydalanilgan funksional kalit k_{f-1} ning xesh-funksiyasi sifatida hisoblab topiladi. Xeshlash kaliti sifatida qoidaga ko'ra shifrlash kalitidan foydalaniladi, xeshlash funksiyasini hisoblash dasturi esa MShAning dastur (yoki apparat) ta'minotiga qo'shib qo'yiladi. Funksional kalitni yangilash davri foydalanilayotgan shifrdan foydalanish rejimi va dastlabki ma'lumotlarning maxfiylik darajasini hisobga olgan holda MShA bayonnomasi bilan belgilanadi.

FOYDALANILGAN ADABIYOTLAR

1. National Institute of Standards and Technology. FIPS PUB 197: Advanced Encryption Standard (AES). Gaithersburg: NIST, 2001.
2. The Design of Rijndael. Joan Daemen, Vincent Rijmen. The Design of Rijndael: AES – The Advanced Encryption Standard. Springer-Verlag, 2002.
3. Understanding Cryptography. Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.
4. Cryptography and Network Security. William Stallings. Cryptography and Network Security: Principles and Practice. 7th Edition, Pearson, 2017.
5. O'z DSt 1105:2009. O'z DSt 1105:2009. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi. Toshkent, 2009.

ISSN 3030-3907