

**MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL**

**MENEJMENT VA IQTISODIYOT
ILMIY-TADQIQOT JURNALI**

**НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ
МЕНЕДЖМЕНТА И ЭКОНОМИКИ**



MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

☎ +998 95 651 90 00

✉ journals@timeedu.uz

📍 Shota Rustaveli ko'chasi, 114

🌐 tmijournals.ndc-agency.uz

✈ @TMII_ilmiy_bolim

Bosh muharrir:

Narbayev Sharafatdin Kengeshovich

Bosh muharrir o'rinbosari:

Nosirova Nargiza Jamoliddin qizi

Muharrir:

Qarshiyeva Shahnoza Davlatovna

Tahrir hay'ati:

1. Sharipov Kongratbay Avezimbetovich – O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vaziri, t.f.d., prof.;
2. Axmedov Xojiakbarxon Dilshatovich – Toshkent menejment va iqtisodiyot instituti rektori i.f.n., dotsent;
3. Gulyamov Saidasror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi, i.f.d, professor;
4. Gulyamov Saidaxror Saidaxmedovich – O'zbekiston Fanlar akademiyasi akademigi i.f.d, professor;
5. Sultanov Mansur Qilichovich – Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi "Inno" innovatsion o'quv-ishlab chiqarish texnoparki bosh direktori, t.f.f.d., dotsent;
6. Chertovitskiy Aleksandr Stepanovich - „Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muxandislari instituti“ Milliy tadqiqot universiteti professori, iqtisodiyot fanlari doktori;
7. Popkova Yelena Gennadyevna - Rossiya Federatsiyasi avtonom notijorat tashkiloti "Ilmiy kommunikatsiyalar instituti" prezidenti, iqtisodiyot fanlari doktori, professor;
8. Dr Goh Khang Wen – Malaziyaning INTI Xalqaro universiteti prorektori;
9. Wang Cheng – XXR "Hebei Institute of Mechanical and Electrical Technology" instituti i.f.f.d., dotsent;
10. Yo'ldoshev Nuriddin Qurbonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
11. Akramov Tohir Abdirahmonovich Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.d., professor;
12. Temirov Abdulaziz Alimjonovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini i.f.n., professor;
13. Rajabov Nazirjon Razzaqovich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini mudiri, i.f.n., dotsent;
14. Xotamov Ibodullo Sadulloyevich – Toshkent menejment va iqtisodiyot instituti Iqtisodiyot kafedrasini i.f.n., professor;
15. Sobirov Aziz Avazbekovich – Toshkent menejment va iqtisodiyot instituti Biznes boshqaruvi va moliya kafedrasini mudiri, i.f.f.d., dotsent;
16. Raximova Shahlo Baxtiyorovna – Ta'lim sifatini nazorat qilish bo'limi boshlig'i, p.f.f.d., dotsent;
17. Kadirova Istora Bobirovna – Toshkent menejment va iqtisodiyot instituti Karyera markazi direktori, i.f.f.d.;
18. Turakulov Otabek Xolmirzayevich – Toshkent menejment va iqtisodiyot instituti Muhandislik va axborot texnologiyalari kafedrasini mudiri, t.f.f.d.

MUHANDISLIK OYLIGI

“RAQAMLI TEXNOLOGIYALARNI RIVOJLANTIRISH VA INNOVATSION MUHANDISLIK YECHIMLARI: ZAMONAVIY TENDENSIYALAR VA ISTIQBOLLAR” MAVZUSIDA RESPUBLIKA ILMIY-AMALIY ANJUMANI TO‘PLAMI MATERIALLARI

17-18 APREL, 2025

TOSHKENT

MUNDARIJA

1.	Primova X.A., Xaniyev N.M., Nodirov M.T. RFID TEXNOLOGIYASI ORQALI OLINGAN MA'LUMOT ASOSIDA QORAMOL KASALLIKLARINI ANIQLASHNING LOYIHALASH	6
2.	Doshanova M.Y., Otaxanova B.I., Aliyev R.R. USING ARTIFICIAL INTELLIGENCE TO AUTOMATE THE PROCESS OF COLLECTING AND ANALYZING DATA FROM ONLINE JOB POSTINGS	10
3.	Eshonqulov E.Sh., Abdiyeva H.S., Abdurahmonov M.S. SUN'IY YO'LDOSH TASVIRLARIDA PANSARPENING YONDASHUVI NATIJALARINI BAHOLASH BAYONNOMALARI	23
4.	Abduraxmanova Z.T. O'ZBEKISTONDA QISHLOQ XO'JALIGINING RAQAMLI TRANSFORMATSIYASI	26
5.	Abdiyeva K.S., Shamsiyeva K., Oblokulov S. GOMPERTZ ALGORITHM FOR THE DETECTION OF BREAST CANCER USING MAMMOGRAPHIC IMAGES	31
6.	Abdiyeva K.S., Shamsiyeva K., Olimjonova S. TOPOGRAPHIC MAP BASED SEGMENTATION OF MEDICAL IMAGES	35
7.	Radjabov B.A. O'ZBEKISTONNING TASHQI SAVDODA LOGISTIKA XARAJATLARI: RAQAMLI YECHIMLAR VA ULARNING EKSPORT RAQOBATBARDOSHLIGIGA TA'SIRI	39
8.	Primova X.A., Vaydullayeva M.F. SUN'IY INTELLEKTNI TALQIN QILISH VA QAROR QABUL QILISH: NORAVSHAN FIKRLASH TIZIMLARINI HISOBLASH MODELLARINI CHUQUR O'RGANISH	49
9.	Ulashov A.E., Obilov H.X. MATEMATIK MASALALARNI ZAMONAVIY DASTURLASH TILLARI YORDAMIDA YECHISH	57
10.	Mamatov N.S., Asqarov A.A. HAVO SIFATI INDEKSINI BASHORATLASHNING REGRESSION MODEL	69
11.	Mirpulatova L.M. AXBOROT TEXNOLOGIYALARI VA RAQAMLI TRANSFORMATSIYANING BANK FAOLIYATIDAGI ROLI	75
12.	Ниезматова Н.А., Жалелов Қ.А., Абдуллаева Б.М. НУТҚ СИГНАЛЛАРИДАН ШОВҚИНЛАРНИ БАРТАРАФ ЭТИШДА ФИЛЬТРЛАР ЖУФТЛИГИНИ ҚЎЛЛАШ ЁНДАШУВИ	84
13.	Mamatov N.S., Jo'rayev I.A., Jalelova M.M., Usarov J.A. TIBBIY TASVIRLAR BAZALARI TAHLILI	88
14.	Mamatov N.S., Jo'rayev I.A., Jalelova M.M., Jumayev B.J. TIBBIY TASVIRLARNI TAHLIL QILISH USUL VA ALGORITMLARI	92
15.	Mamatov N.S., Jalelova M.M., Jo'rayev I.A., Turakulova Sh.A. TIBBIY 2D TASVIRLAR ASOSIDA 3D TASVIRLARNI SHAKLLANTIRISH USULLARI	96
16.	Niyozmatova N.A., Madaminjonov A.D. INSON HIS-TUYG'ULARINI ANIQLASH DASTURIY VOSITALARI VA QURILMALARI	99

17.	Мухамедиева Д.Т., Маматов Н.С., Маматов А.А. МАТНЛИ МАЪЛУМОТЛАРНИ ТАСНИФЛАШДА БЕЛГИЛАРНИ ШАКИЛЛАНТИРИШ УСУЛ ВА АЛГОРИТМЛАРИ	103
18.	Raximov M. KASB KOMPETENSIYASIDA RAQAMLI TA'LIM TRANSFORMATSIYASI	106
19.	Turakulov O.X. MATNLI MA'LUMOTLARNI QAYTA ISHLASH BOSQICHLARI	110
20.	Turakulov O.X., Jalelov R.M. MATNLI MA'LUMOTLARGA DASTLABKI ISHLOV BERISH ALGORITMLARI	116
21.	Мухамедиева Д.К. ПОСТРОЕНИЕ ДЕРЕВА МЕРКЛА	123
22.	Mamatov N.S., Nuritdinov N.D., Almuradova N.A. IJTIMOIY TIZIMLARDA RAQAMLI TRANSFORMATSIYA JARAYONLARINI MODELLASHTIRISH	127
23.	Kabildjanov A.S., Pulatov G'.G. OB-HAVO OMILLARINING YURAK-QON TOMIR KASALLIKLARIGA TA'SIRINING SUN'IY INTELLEKT ASOSIDA TAHLILI	130
24.	Mamatov N.S., Kodirov E.S KAFT TASVIRI ASOSIDA SHAXSNI TANIB OLIH YONDASHUVLARI TAHLILI	133
25.	Raximov I.M. MAHALLIY ISHLAB CHIQUVCHILARNING XALQARO STANDARTLARGA MOSLASHUVI – IMKONIYATLAR, YUTUQLAR VA BARQAROR STRATEGIK YECHIMLAR	136
26.	Raximov F.J. TABIIY VA SUN'IY TOLALAR ASOSIDA QAYTA ISHLANGAN MAHSULOTLARNING TEXNOLOGIK SIFATI VA IQTISODIY SAMARADORLIGI	143
27.	Mamatov N.S., Dusanov X.T. NUTQ SIGNALINI XALAQITLARDAN TOZALASH USULLARI	150
28.	Dauletov A.Y., Sabirova S.T., Oydinov S.SH. ARXIVDA MATNLARNI QIDIRISH USULLARI TAHLILI	155
29.	Toshpulatov M. UNVEILING TOMORROW: EXPLORING THE FRONTIERS OF INNOVATION	162
30.	Маматов Н.С., Ниёзматова Н.А., Тожибоева Ш.Х., Яхяев Б.Ю., Машанпин Т.В. ИНСОН ҲИС-ТУЙҒУЛАРИНИ ЮЗ ТАСВИРИ ОРҚАЛИ АНИҚЛАШ ДАСТУРИЙ ВОСИТАЛАРИ ВА ҚУРИЛМАЛАРИ	165
31.	Ниёзматова Н.А., Маматов Н.С., Турғунова Н.М. МАТНЛИ МАЪЛУМОТЛАРНИ ТАСНИФЛАШ УСУЛ ВА АЛГОРИТМЛАРИ ТАҲЛИЛИ	172
32.	Маматов Н.С., Валижонов И.Х., Шукруллоев Б.Р. ТАСВИРЛАРНИ ТАСНИФЛАШДА ҚўЛЛАНИЛАДИГАН УСУЛЛАР	185
33.	Niyozmatova N.A., Xoitqulov A.A., Mamatov A.A. MATNLI MA'LUMOTLARDAN FAKTLARNI AJRATISH TEXNOLOGIYALARI	178
34.	Buribaeva Z.R. DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE IN EDUCATION: CHALLENGES AND OPPORTUNITIES	181

35.	Anarova Sh.A., Ibrohimova Z.E., Boliyeva D.N. R-FUNKSIYA USULINI (RFM) QO'LLAGAN HOLDA KO'P O'LCHOVLI FRAKTAL TUZILISHDAGI TASVIRLARNI GEOMETRIK MODELLARINI ISHLAB CHIQUISH	188
36.	Ibrohimova Z.E., Qarshiboyev J.O', Xaniyev N.M. KOMPYUTER GRAFIKASINING GEOMETRIK ALMASHTIRISHLARI ASOSIDA MURAKKAB FRAKTAL TUZILISHLARNI MATEMATIK VA RAQAMLI MODELLASHTIRISHNI AMALGA OSHIRISH	192
37.	Xalimov A.A. SANOAT KORXONALARIDA QAYTA TIKLANUVCHI ENERGIYA MANBALARIDAN FOYDALANISH YO'LLARI	198
38.	Rustamova M.M. INNOVATIVE TECHNOLOGIES AND INVESTMENT EFFICIENCY IN COTTON- TEXTILE CLUSTERS: OPTIMIZING COSTS THROUGH INDUSTRY 4.0 SOLUTIONS.	204
39.	Suyarov A.M. AXBOROTLARNI VIZUAL TAQDIM ETISHDA INFOGRAFIKA VOSITALARINI YARATISH USULLARI	214
40.	Saminjonov N.A. CHAKANA SAVDO FAOLIYATIDA RAQAMLI VA NEYROMARKETING STRATEGIYALARINING INTEGRATSIYASI	219
41.	Alimov A.A. INDUSTRY 4.0 TALABLARI ASOSIDA MUHANDISLIK TA'LIMINI TASHKIL ETISH MASALALARI	224
42.	Sobirov A.A., Zaripbayeva A.A. SANOAT KLASSTERLARINI SHAKLLANISH MEXANIZMLARI VA ZAMONAVIY MODELLARI	228
43.	Sharipov K.A., Karimov V.A. AQLLI ENERGIYA TIZIMLARI VA QAYTA TIKLANADIGAN ENERGIYA MANBALARIDAN FOYDALANISH USULLARI VA SAMARADORLIGI	237
44.	Маматов Н.С., Самижонов А.Н., Самижонов Б.Н. ИНСОН ЭХТИЁЖЛАРИНИ АНГЛОВЧИ ВА УЛАРГА ЖАВОБ БЕРИШ ҚОБИЛИЯТИГА ЭГА ЭМПАТИК РОБОТЛАР	246
45.	Yusupov R.A., G'ulomov A.X. MAYSALARNI O'RISH VA QOR TOZALASH MASHINASINI MASOFADAN BOSHQARISHNI AVTOMATLASHTIRISH	251
46.	Yusupov R.A., Qurbonov Sh.B. HELIX: FOYDALANUVCHIGA MOSLASHA OLADIGAN, KUNDALIK HAYOTDA YORDAM BERUVCHI SUN'IY INTELLEKT	254
47.	Haydarov E.D., Dusmurodov Q.A. OCHIQ WI-FI TARMOQLAR XAVFSIZLIGI	257
48.	Haydarov E.D., Dusmurodov Q.A. SIMSIZ TARMOQDA XAVFSIZLIK	265
49.	Ro'ziyeva F.K. MAISHIY KIMYO TOVARLARI B2B TAQSIMOTIDA KO'P KANALLI MARKETING STRATEGIYASINING AHAMIYATI	269
50.	Qudratov U.I., Abdullayeva N.R. MASHINANI O'QITISH USULLARIDAN FOYDALANGAN HOLDA ZARARLI DASTURLARNI ANIQLASH	277

51.	Muhamediyeva D.T., Raupova M. ELLIPTIK EGRI CHIZIQ ASOSIDA XAVFSIZ KALIT ALMASHINUVI	279
52.	Muhamediyeva D.T., Raupova M. POST-KVANT KRIPTOGRAFIYA ASOSIDA POLINOMLAR BILAN SHIFRLASH	282
53.	Muhamediyeva D.T., Raupova M. KVANT KALIT ALMASHINUVI BILAN INTEGRATSIYALANGAN RSA SHIFRLASH	285
54.	Mamayusupov A.A. ZAMONAVIY RAQAMLI MUHITDA KIBERXAVFSIZLIK TAHDIDLARI VA ULARNING OLDINI OLISH YO'LLARI	288
55.	Тоиров Ш. А. ОПТИМИЗАЦИЯ ФУНКЦИЙ С ПРИМЕНЕНИЕМ ЭВОЛЮЦИОННЫХ АЛГОРИТМОВ	291
56.	Toirov Sh. A. ARCHITECTURE OF OPERATORS IN QUANTUM ALGORITHMS	397
57.	Olimov S.A. TALABALARNING O'ZLASHTIRISH NATIJALARINI BAHOLASHDA RAQAMLI TEXNOLOGIYALARNING O'RNI	302
58.	Olimov S.A. OLIIY TA'LIM MUASSASALARIDA O'QUV JARAYONINI BOSHQARISHDA RAQAMLI TEXNOLOGIYALARNING AHAMIYATI	309
59.	Uzakova G.Z. ENGAGING ESP LEARNERS: STRATEGIES FOR PRODUCTIVE LESSONS	316
60.	Shafkarov F.X. SANATORIY-SOQ'LOMLASHTIRISH MUASSASALARINING ICHKI AUDITINI FUNDAMENTAL ASOSDA TASHKIL ETISH	321
61.	Raximov Sh.F. TIJORAT BANKLARIDA MIJOZLARNING SODIQLIK DASTURLARI ASOSIDA DEPOZITLARNI OSHIRISH YO'LLARI	329
62.	Туракулова Ш.А., Суюнова Н. ОПИСАНИЕ КРАЙНИХ ГИББОВСКИХ МЕР ДЛЯ МОДЕЛИ ИЗИНГА С НЕНУЛЕВЫМ ВНЕШНИМ МАГНИТНЫМ ПОЛЕМ НА РЕШЕТКЕ БЕТЕ	337
63.	Ulashov A.E. ZAMONAVIY TA'LIM TIZIMINING RAQAMLI TRANSFORMATSIYASI: TENDENSIYALAR, MUAMMOLAR VA YECHIMLARI	344
64.	Radjabov B.A. O'ZBEKISTONDA TA'LIMNING RAQAMLI TRANSFORMATSIYASI VA SUN'IY INTELLEKT	353
65.	Mamatov N.S., Ibroximov S.R., Almuradova N.A. O'QUV JARAYONIDA SUN'IY INTELLEKT VOSITALARIDAN FOYDALANISH	359
66.	Kuvandikov J.T., Tojiyev A.H. Axborot resurslaridan foydalanish ko'rsatkichlarini normallashtirish asosida bilim oluvchilarning bilim darajasini obyektiv baholash usullari	364
67.	Saidov S.F. TA'LIMDA SUN'IY INTELLEKTDAN SAMARALI FOYDALANISH MASALALARI	374
68.	Suyunova N.A. TA'LIMDA MANTIQ TUSHUNCHASI VA O'QUVCHILARDA MANTIQUIY FIKRLASHNI RIVOJLANTIRISHNING INNOVATSION TEXNOLOGIYALARI	382

69.	Kuvandikov J.T. Tojiyev A.H. TA'LIM OLUVCHILAR BILIMINI BAHOLASHDA NORAVSHAN MANTIQDAN FOYDALANISH	389
70.	Djabbarova M.D. KASB-HUNAR TA'LIMIDA ELEKTRON TA'LIMNING PEDAGOGIK VA PSIXOLOGIK ASOSLARI	393
71.	Anarkulova G.M., Abduraxmanova F.N. OLIIY TA'LIMDA MAXSUS FANLAR BO'YICHA MASHG'ULOTLARDA ISHCHAN VA ROLLI O'YINLAR METODINI QO'LLASH INNOVATSION YONDASHUV	396
72.	Анаркулова Г.М., Абдиганиева З.С. ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ И НАВЫКОВ СТУДЕНТОВ КАК ФАКТОР УСПЕВАЕМОСТИ	406
73.	Obidov R.A. TA'LIMDA KEYS TEXNOLOGIYALARINING AHAMIYATI	417
74.	Narbayev Sh.K., Maxkamova N.X. MAXSUS FANLARNI O'QITISHDA RAQAMLI VA INNOVATSION TEXNOLOGIYALARIDAN FOYDALANISHNING METODIK SHART-SHAROITLARI	422
75.	Erhanova N.A. MAKTABGACHA TA'LIM TASHKILOTLARIDA MULTIMEDIA RESURSLARIDAN FOYDALANISH SAMARADORLIGI	430
76.	Xidoyatov M.B. OLIIY TA'LIM MUASSASALARIDA RAQAMLI MARKETING FAOLIYATINI BAHOLASH: AXBOROT TEXNOLOGIYALARIGA ASOSLANGAN YONDASHUVLAR	435
77.	Темиров А.А. АКЦИЯДОРЛИК ЖАМИЯТЛАРИ ФАОЛИЯТИГА РАҚАМЛИ БОШҚАРУВНИ ЖОРИЙ ЭТИШ ИСТИҚБОЛЛАРИ	444
78.	В.А.Ахмадалиев ЧОРВАЧИЛИК ХЎЖАЛИКЛАРИНИ ТАШКИЛ ЭТИШ ВА УЛАРГА ЕР АЖРАТИШ ТАРТИБИ	454
79.	Носирова Н.Дж. ЭКСПОРТНЫЙ ПОТЕНЦИАЛ СУБЪЕКТОВ МАЛОГО БИЗНЕСА УЗБЕКИСТАНА: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ (2018–2025 ГГ)	459
80.	Матлюбов Х.Ж. ТРАНСФОРМАЦИЯ ПРОМЫШЛЕННОЙ ПОЛИТИКИ: ОСНОВНЫЕ ТЕНДЕНЦИИ И ВЫЗОВЫ	463
81.	Sa'dulloyev H. I. SANOAT KORXONALARINING EKO-MARKETING TIZIMINI BAHOLAH AMALIYOTI	469

POST-KVANT KRIPTOGRAFIYA ASOSIDA POLINOMLAR BILAN SHIFRLASH

¹Muhamediyeva D.T., ²Raupova M.

¹"Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" Milliy tadqiqot universiteti,

²Chirchiq davlat pedagogika universiteti,

Annotatsiya. Ushbu maqolada NTRU (N-th degree Truncated Polynomial Ring) shifrlash algoritmi taqdim etiladi va polinomlar yordamida shifrlash va deshifrlash jarayonlari kengaytiriladi. Shifrlash va deshifrlash algoritmlarining ishlashi, tasodifiy polinomlar yaratish va xabarlarni polinomlarga aylantirish orqali amalga oshiriladi. Maqolada NTRU algoritmining kvantga chidamli xususiyatlari va u qanday qilib klassik RSA yoki elliptik egri algoritmlaridan farq qilishi haqida muhokama qilinadi.

Kalit so'zlar: NTRU shifrlash, Post-quantum cryptography, Polinomlar bilan shifrlash, Kvantga chidamli algoritmlar, Xavfsiz kalit almashish

Abstract. This paper presents the NTRU (N-th degree Truncated Polynomial Ring) encryption algorithm and extends the encryption and decryption processes using polynomials. The encryption and decryption algorithms work by generating random polynomials and converting messages into polynomials. The paper discusses the quantum-resistant properties of the NTRU algorithm and how it differs from classical RSA or elliptic curve algorithms.

Keywords: NTRU encryption, Post-quantum cryptography, Polynomial encryption, Quantum-resistant algorithms, Secure key exchange

Аннотация. В данной статье представлен алгоритм шифрования NTRU (усеченное полиномиальное кольцо N-й степени) и расширены процессы шифрования и дешифрования с использованием полиномов. Работа алгоритмов шифрования и дешифрования осуществляется путем генерации случайных полиномов и преобразования сообщений в полиномы. В статье рассматриваются квантово-устойчивые свойства алгоритма NTRU и его отличия от классических алгоритмов RSA или эллиптических кривых.

Ключевые слова: шифрование NTRU, постквантовая криптография, полиномиальное шифрование, квантово-устойчивые алгоритмы, безопасный обмен ключами

Kirish.

Post-kvant kriptografiyaga oid asosiy yo'nalishlar va ularning qisqacha tavsifi, shuningdek Python orqali soddalashtirilgan namunaviy kod bilan bir nechtasini ko'rib chiqamiz. Bu algoritmlar Shor algoritmiga chidamli bo'lib, kelajakdagi kvant kompyuter hujumlariga bardosh bera oladi.

NTRU shifrlash algoritmi xabarlarni polinomlar bilan shifrlashni ta'minlaydi va bu algoritmning xavfsizligi polinomlar va ularning ko'paytmasiga asoslangan matematik muammolarga bog'liq. Shifrlash va deshifrlash jarayonlarida polinomlar ustida arifmetik operatsiyalarni bajarish orqali, shifrlangan xabarni

faqat maxfiy kalitga ega bo'lgan tomonlar deshifrlay oladi.

2. Usullar. NTRU algoritmi post-quantum kriptografiyasida ishlatiladigan eng samarali va xavfsiz tizimlardan biridir. NTRU shifrlashning asosiy tamoyili polinomlar ustida ishlashga asoslanadi. Ushbu bo'limda, NTRU shifrlash va deshifrlash jarayonlari, shuningdek, bu tizimning matematik formulalarini ko'rib chiqamiz.

NTRU algoritmda kalitlar polinomlar ustida quriladi. Biz ikki xil kalitni yaratamiz: ochiq kalit va maxfiy kalit.

1. Maxfiy kalit f, g ikkita polinomdan iborat bo'ladi:

$$f(x) = f_0 + f_1x + f_2x^2 + \dots + f_Nx^N$$

$$g(x) = g_0 + g_1x + g_2x^2 + \dots + g_Nx^N$$

Bu polinomlar kichik butun sonlar bilan ifodalanadi va ularning o'zaro teskari bo'lishi talab etiladi.

2. Ochiq kalit $h(x)$ quyidagi shaklda bo'ladi:

$$h(x) = f^{-1}(x) \cdot g(x) \mod q$$

Bu yerda $f^{-1}(x)f(x)$ ning modulyar teskari polinomi bo'lib, q esa xavfsizlikni ta'minlash uchun tanlangan katta son hisoblanadi.

Shifrlash jarayonida yuboruvchi (masalan, Alice) xabarni $m(x)$ polinomi sifatida ifodalaydi va bu xabarni quyidagi formula yordamida shifrlaydi:

1. Xabarni polinom shaklida ifodalash:

$$m(x) = m_0 + m_1x + m_2x^2 + \dots + m_Nx^N$$

Xabar $m(x)$ uzunligi N -ni tashkil qiladi va faqat kichik butun sonlar bilan ifodalanadi.

2. Shifrlashda yuboruvchi $e(x)$ va $r(x)$ tasodifiy polinomlarni tanlaydi. Shifrlash uchun quyidagi formulani qo'llaymiz:

$$c_1(x) = r(x) \cdot h(x) \mod q$$

$$c_2(x) = m(x) + r(x) \cdot f(x) \mod q$$

Bu yerda $c_1(x)$ va $c_2(x)$ shifrlangan xabarni tashkil etadi.

3. Natijalar. Ushbu maqolada, NTRU algoritmi yordamida shifrlash va deshifrlash jarayonlari amalga oshirildi. Kutilgan natijalar quyidagicha:

Ochiq

kalit:00001021211000000102121100
0000102121100

Ochiq kalit $h(x)$, polinomlar ustida qurilgan va xavfsizlikni ta'minlash uchun maxfiy kalit bilan bog'langan. Maxfiy kalit: $[[0,1,0,0,1,1,1],[0,0,1,0,1,1,1]]([0, 1, 0, 0, 1, 1, 1], [0, 0, 1, 0, 1, 1, 1])$

Maxfiy kalit $f(x)$ va $g(x)$ polinomlarining qiymatlari, bu polinomlar yordamida xabarni shifrlash va deshifrlash amalga oshiriladi.

Shifrlangan matn (c_1 va c_2):
0000000001124363523110000,
1101001

Shifrlash jarayonida $m(x)$ xabarini tasodifiy polinomlar yordamida shifrlash natijasida olingan c_1 va c_2 polinomlaridir. Deshifrlangan matn:1101001

3. Xulosa. Ushbu maqolada NTRU (Number Theoretic Transform Unit) algoritmi asosida kriptografik tizimni yaratish va uning kvantga

chidamli xususiyatlarini ko'rib chiqdik. NTRU algoritmi, uning polinomial asosidagi shifrlash va deshifrlash metodlari yordamida xavfsiz kalit almashinuvi va xabarni himoya qilish

imkoniyatlarini taqdim etadi. Dasturda maxfiy va ochiq kalitlar generatsiyasi, shifrlash va deshifrlash jarayonlari muvaffaqiyatli amalga oshirildi.

Foydalanilgan adabiyotlar ro'yxati:

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2017.
2. R. K. Santosh, M. S. Arumugam, and M. B. W. Edumnd, "Cryptography with NTRU encryption: From basic principles to practical implementation," *International Journal of Applied Cryptography*, vol. 12, no. 5, pp. 35–50, 2021.
3. P. Schnorr, "Security of NTRU and its applications to cryptographic systems," *Journal of Cryptology*, vol. 25, pp. 452–487, 2016. <https://doi.org/10.1007/s00145-015-9223-4>.

Ingliz tili muharriri: Nosirova Nargiza Jamoliddin qizi
Musahhih: Vahobova Marfua Mirkamalovna
Sahifalovchi va dizayner: Zoirov Sardor Ziyodin o'g'li

1-maxsus son

© Materiallar ko'chirib bosilganda **"Management and Economics Scientific Research Journal"** jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pullik asosda chop etiladi.

El. pochta: journals@timeedu.uz

Tel.: [+998 95 651 90 00](tel:+998956519000)

"Management and Economics Scientific Research Journal" jurnali 19.09.2024-yildan O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: Toshkent shahar, Yakkasaroy tumani
Shota Rustaveli ko'chasi, 114