KRIPTOGRAFIK ALGORITMLAR VA SONLAR NAZARIYASINING ZAMONAVIY QO‘LLANILISHI

Izboskan tuman 2-son Texnikumi
Matematika fani o‘qituvchisi
Xidirova Barchinoy Tolibovna

Annotatsiya

Ushbu maqolada kriptografik algoritmlar hamda sonlar nazariyasining zamonaviy axborot-kommunikatsiya tizimlaridagi o‘rni IMRAD talabi asosida tahlil qilinadi. Raqamli iqtisodiyot, elektron hukumat, bank-moliya xizmatlari, bulutli texnologiyalar, elektron raqamli imzo va blokcheyn muhitida ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlash kriptografiyaga tayanadi. Sonlar nazariyasi esa tub sonlar, modular arifmetika, diskret logarifm, elliptik egri chiziqlar, qoldiqlar sinflari va murakkablik nazariyasi orqali zamonaviy algoritmlarning matematik poydevorini tashkil etadi. Tadqiqotda RSA, Diffie-Hellman, ElGamal, AES, SHA oilasi, elliptik egri chiziqlar kriptografiyasi va post-kvant algoritmlarining amaliy xususiyatlari qiyosiy ko‘rib chiqildi. O‘zbekiston Respublikasida kiberxavfsizlik, axborotni kriptografik himoyalash va kriptologiya sohasidagi ta’lim-ilmiy maktabni rivojlantirishga qaratilgan normativ-huquqiy islohotlar mavzuning milliy dolzarbligini kuchaytiradi.

Kalit so‘zlar: kriptografiya, sonlar nazariyasi, RSA, elliptik egri chiziqlar, modular arifmetika, elektron raqamli imzo, post-kvant kriptografiya, kiberxavfsizlik, autentifikatsiya, axborotni himoyalash.

СОВРЕМЕННЫЕ ПРИМЕНЕНИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ И ТЕОРИИ ЧИСЕЛ

Аннотация

В статье на основе структуры IMRAD анализируется современное применение криптографических алгоритмов и теории чисел в информационно-коммуникационных системах. В условиях цифровой экономики, электронного правительства, банковских услуг, облачных платформ, электронной цифровой подписи и блокчейна конфиденциальность, целостность и подлинность данных обеспечиваются криптографическими механизмами. Теория чисел формирует математическую основу современных алгоритмов через простые числа, модульную арифметику, дискретный логарифм, эллиптические кривые, классы вычетов и теорию сложности.

Ключевые слова: криптография, теория чисел, RSA, эллиптические кривые, модульная арифметика, электронная цифровая подпись, постквантовая криптография, кибербезопасность, аутентификация, защита информации.

MODERN APPLICATIONS OF CRYPTOGRAPHIC ALGORITHMS AND NUMBER THEORY

Abstract

This article examines the modern application of cryptographic algorithms and number theory in information and communication systems according to the IMRAD structure. In the digital economy, e-government, banking, cloud computing, digital signatures and blockchain environments, confidentiality, integrity and authentication rely on cryptographic mechanisms. Number theory provides the mathematical foundation of modern algorithms through prime numbers, modular arithmetic, discrete logarithms, elliptic curves, residue classes and computational complexity. The study compares RSA, Diffie-Hellman, ElGamal, AES, SHA families, elliptic curve cryptography and post-quantum cryptographic approaches.

Keywords: cryptography, number theory, RSA, elliptic curves, modular arithmetic, digital signature, post-quantum cryptography, cybersecurity, authentication, information protection.

Kirish

Raqamli transformatsiya jarayonlari jamiyatning barcha sohalarida axborot almashinuvi tezligini oshirdi, ammo bu jarayon ma’lumotlarning noqonuniy qo‘lga kiritilishi, o‘zgartirilishi va soxtalashtirilishi bilan bog‘liq xavflarni ham kuchaytirdi. Elektron hukumat portallari, masofaviy bank xizmatlari, elektron tijorat, tibbiy axborot tizimlari, ta’lim platformalari va korporativ tarmoqlarda axborot xavfsizligi endilikda faqat texnik masala emas, balki davlat boshqaruvi, iqtisodiy barqarorlik va fuqarolarning konstitutsiyaviy huquqlarini himoya qilish bilan bog‘liq strategik yo‘nalish sifatida qaralmoqda.

Kriptografik algoritmlar axborotni shifrlash, raqamli imzolash, foydalanuvchini autentifikatsiya qilish, kanal xavfsizligini ta’minlash va ma’lumot yaxlitligini nazorat qilishning asosiy vositasidir. Mazkur algoritmlar tub sonlarni faktorizatsiyalash, chekli maydonlarda diskret logarifmni hisoblash, elliptik egri chiziqlardagi algebraik guruhlar, xesh-funksiyalarning kolliziya barqarorligi va boshqa matematik murakkab masalalarga asoslanadi. Shu bois kriptografiya amaliy dasturlash bilan bir qatorda sonlar nazariyasi, algebra, ehtimollar nazariyasi va hisoblash murakkabligi nazariyasi bilan bevosita bog‘langan fanlararo sohaga aylandi.

O‘zbekiston Respublikasida kiberxavfsizlik va axborotni kriptografik himoyalash davlat siyosatining muhim tarkibiy qismiga aylanmoqda. “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonunda kiberxavfsizlikni ta’minlashda axborotni kriptografik va texnik jihatdan himoya qilish choralariga alohida e’tibor qaratiladi. Prezident Shavkat Mirziyoyevning 2024-yil 15-avgustdagi PQ-293-son qarori esa O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha yangi institutsional bosqichni

belgilab berdi. Ushbu hujjatda kriptografiya va kriptotahlil bo‘yicha yuqori malakali kadrlar tayyorlash, ilmiy maktablarni shakllantirish hamda axborotni kriptografik himoyalash salohiyatini oshirish vazifalari belgilangan.

Mavzuning dolzarbligi kvant hisoblash texnologiyalarining rivojlanishi bilan yanada ortmoqda. Hozirgi ochiq kalitli kriptotizimlarning muhim qismi faktorizatsiya va diskret logarifm masalalariga tayanadi. Yetarlicha quvvatli kvant kompyuterlar paydo bo‘lganda Shor algoritmi bunday tizimlar uchun jiddiy xavf tug‘dirishi mumkin. Shu sababli AQSH Milliy standartlar va texnologiyalar instituti 2024-yilda ML-KEM, ML-DSA va SLH-DSA kabi post-kvant standartlarini e’lon qildi. Yevropa davlatlari, MDH mamlakatlari va Osiyo mintaqasidagi ilmiy markazlar ham kvantga bardoshli algoritmlar, milliy kriptografik standartlar va xavfsiz kalit infratuzilmasi ustida izlanishlar olib bormoqda.

Metodologiya

Yevropa ilmiy maktablari doirasida kriptografiya ko‘proq standartlashtirish, elektron identifikatsiya, ma’lumotlarni himoyalash reglamentlari va post-kvant migratsiya masalalari bilan bog‘liq holda o‘rganilmoqda. Belgiyalik olimlar Jean-Jacques Quisquater va Bart Preneel, Germaniyalik Johannes Buchmann, Daniyalik Ivan Damgård, Buyuk Britaniyalik Nigel Smart hamda Steven Galbraithning ishlari kriptografik protokollar, elliptik egri chiziqlar, raqamli imzo va amaliy xavfsizlikni baholashda muhim ahamiyatga ega. Yevropa Ittifoqining ENISA tavsiyalari post-kvant algoritmlarini bosqichma-bosqich joriy etish, kriptografik inventarizatsiya va xavfga asoslangan migratsiyani taklif qiladi.

MDH davlatlarida kriptografiya milliy standartlar, davlat axborot resurslari xavfsizligi va elektron hujjat aylanishi bilan bog‘langan holda rivojlangan. Rossiya ilmiy maktabida A. A. Moldovyan, N. D. Moldovyan, V. M. Sidelnikov, I. B. Fomichev, V. K. Zadiraka kabi tadqiqotchilar kriptografik algoritmlar, xesh-funksiyalar, blokli shifrlar va kriptotahlil nazariyasini rivojlantirishga hissa qo‘shgan. Qozog‘iston, Belarus va boshqa MDH mamlakatlarida ham davlat

standartlari, elektron raqamli imzo infratuzilmasi va axborot xavfsizligi ta'limi bo'yicha tadqiqotlar olib boriladi.

O'zbekiston tajribasida kriptologiya sohasining rivoji kiberxavfsizlik siyosati, raqamli iqtisodiyot va axborot tizimlarini himoya qilish ehtiyoji bilan bevosita bog'liq. Mamlakat oliy ta'lim muassasalarida axborot xavfsizligi, kiberxavfsizlik injiniringi, kriptografiya va kriptotahlil yo'nalishlari bo'yicha kadrlar tayyorlanmoqda. O'zbek olimlari va mutaxassislari tomonidan axborot xavfsizligi, elektron raqamli imzo, kriptografik protokollar, tarmoqlar xavfsizligi va raqamli texnologiyalarni himoyalash masalalari o'rganilmoqda. Mahalliy tadqiqotlarda milliy kriptografik vositalarning ishonchliligi, davlat axborot tizimlarida kalitlarni boshqarish, foydalanuvchi identifikatsiyasi va xavfsiz autentifikatsiya masalalari alohida ahamiyat kasb etadi.

Tadqiqot natijalari

Tahlil natijalari kriptografik algoritmlarning xavfsizligi algoritm nomi yoki dasturiy kutubxona bilan emas, balki matematik asos, kalit uzunligi, parametrlar sifati, tasodifiy sonlar generatori, protokol dizayni va amaliy joriy etish madaniyati bilan belgilanadi. RSA algoritmida xavfsizlik katta sonlarni tub ko'paytuvchilarga ajratish masalasining murakkabligiga tayanadi. Amaliy tizimlarda 2048 bit va undan yuqori kalitlar minimal xavfsizlik talabi sifatida qaraladi, ammo uzoq muddatli maxfiylik uchun post-kvant tahdidlarini ham inobatga olish zarur.

Diffie-Hellman va ElGamal algoritmlarida diskret logarifm masalasi asosiy xavfsizlik tayanchi hisoblanadi. Chekli maydonlarda yoki elliptik egri chiziqlarda diskret logarifmni hisoblash klassik kompyuterlar uchun murakkab bo'lgani sababli mazkur algoritmlar xavfsiz kanal hosil qilishda keng qo'llanadi. Elliptik egri chiziqlar kriptografiyasi an'anaviy RSAga nisbatan kichikroq kalitlar bilan taqqoslanadigan xavfsizlik darajasini berishi sababli mobil qurilmalar, IoT tizimlari va resursi cheklangan muhitlar uchun qulaydir.

Sonlar nazariyasi kriptografik barqarorlikni ta’minlovchi asosiy matematik qatlam sifatida namoyon bo‘ladi. Tub sonlar tasodifiy tanlanmasa yoki tekshiruv yetarli darajada bajarilmasa, RSA moduli zaiflashadi. Modular arifmetika xatolari, qayta ishlatilgan nonce qiymatlari, yomon entropiya va protokol bosqichlarining noto‘g‘ri bajarilishi kriptografik tizimlarni nazariy jihatdan kuchli bo‘lsa ham amalda zaiflashtiradi. Shu jihatdan sonlar nazariyasi algoritmni yaratishda ham, uning kriptotahlilini baholashda ham zarur ilmiy vosita hisoblanadi.

Post-kvant kriptografiya natijalari shuni ko‘rsatadiki, kelajakdagi xavfsiz tizimlar faqat RSA yoki elliptik egri chiziqlarga tayanib qolmasligi kerak. ML-KEM kalit kapsulyatsiyasi, ML-DSA raqamli imzo va SLH-DSA xeshga asoslangan imzo usullari kvantga bardoshli migratsiyaning asosiy yo‘nalishlari sifatida e’tirof etilmoqda. Bunday algoritmlarning joriy etilishi mavjud sertifikat infratuzilmasi, elektron hujjat aylanishi, bank tizimlari, davlat axborot resurslari va bulutli xizmatlarda bosqichma-bosqich inventarizatsiya, sinov va standartlashtirishni talab qiladi.

Muhokama

Kriptografik algoritmlarning zamonaviy qo‘llanilishi axborot xavfsizligining uch asosiy tamoyili - maxfiylik, yaxlitlik va mavjudlik bilan bog‘liq. Maxfiylik shifrlash algoritmlari orqali, yaxlitlik xesh-funksiyalar va xabar autentifikatsiya kodlari orqali, ishonchlilik esa raqamli imzo va sertifikat infratuzilmasi orqali ta’minlanadi. Bank ilovalari, davlat xizmatlari portallari, masofaviy ta’lim platformalari va korporativ tizimlar ushbu mexanizmlarsiz ishonchli ishlay olmaydi.

Raqamli hujjat aylanishida elektron raqamli imzo alohida ahamiyatga ega. Imzo egasini identifikatsiya qilish, hujjat o‘zgarmaganligini tasdiqlash va mualliflikdan voz kechishning oldini olish funksiyalari davlat boshqaruvi hamda biznes jarayonlarining huquqiy ishonchliligini ta’minlaydi. Bu jarayonda kriptografik kalitlarning maxfiy saqlanishi, sertifikatlarning amal qilish muddati,

bekor qilingan sertifikatlar ro‘yxati va imzo algoritmlarining yangiligi muhim shart hisoblanadi.

Blokcheyn texnologiyalarida sonlar nazariyasi va kriptografiya xesh zanjirlari, elektron imzolar, konsensus mexanizmlari va manzillar hosil qilish jarayonida qo‘llanadi. Kriptografik xesh-funksiyaning bir tomonlama xususiyati bloklar zanjirini o‘zgartirishni iqtisodiy va hisoblash jihatdan qimmatlashtiradi. Elektron imzo esa tranzaksiyani tasdiqlash hamda foydalanuvchi mulk huquqini matematik dalil bilan mustahkamlash imkonini beradi.

Kiberxavfsizlik amaliyotida eng katta xatolardan biri kuchli algoritmning o‘zi yetarli degan tasavvurdir. Amalda zaif parollar, eskirgan protokollar, noto‘g‘ri sertifikat sozlamalari, xavfsiz bo‘lmagan tasodifiy sonlar generatori, kalitlarni oddiy faylda saqlash yoki ishlab chiqarish muhitida test kalitlardan foydalanish kabi omillar eng zamonaviy kriptografiyani ham samarasiz qiladi. Shuning uchun kriptografiyani joriy etishda standartlar, audit, xavfsizlik siyosati va kadrlar malakasi birgalikda ko‘rilishi lozim.

Xulosa

Kriptografik algoritmlar va sonlar nazariyasining zamonaviy qo‘llanilishi raqamli jamiyat xavfsizligining ilmiy, texnik va huquqiy asoslarini birlashtiruvchi muhim yo‘nalishdir. Bugungi kunda ma’lumotlar qiymati ortib borayotgan sharoitda axborotni shifrlash, elektron raqamli imzo bilan tasdiqlash, foydalanuvchini ishonchli autentifikatsiya qilish, kalitlarni boshqarish va ma’lumot yaxlitligini tekshirish har qanday raqamli platformaning zarur funksiyasiga aylandi. Mazkur funksiyalar zamirida esa sonlar nazariyasining tub sonlar, modular arifmetika, diskret logarifm, elliptik egri chiziqlar va hisoblash murakkabligi kabi tushunchalari yotadi.

Tahlillar shuni ko‘rsatdiki, kriptografik xavfsizlik algoritm tanlash bilan cheklanmaydi. Algoritm matematik jihatdan barqaror bo‘lishi, standart parametrlar bilan ishlatilishi, to‘g‘ri protokolga joylashtirilishi, kalitlar hayotiy sikli nazorat

qilinishi va foydalanuvchi muhitida xavfsiz amalga oshirilishi kerak. RSA, Diffie-Hellman, ElGamal va elliptik egri chiziqlar klassik ochiq kalitli kriptografiyaning asosini tashkil etsa, AES va xesh-funksiyalar katta hajmli ma'lumotlar oqimini himoyalashda amaliy jihatdan samarali hisoblanadi. Shu bilan birga, kvant hisoblash texnologiyalari mavjud tizimlar uchun uzoq muddatli xavf yaratgani sababli post-kvant kriptografiyaga o'tish strategik zaruratga aylanmoqda.

Umumiy xulosa sifatida aytish mumkinki, kriptografik algoritmlar raqamli ishonch infratuzilmasining yuragi, sonlar nazariyasi esa uning matematik asosi hisoblanadi. Kelajakda xavfsiz raqamli davlat, elektron iqtisodiyot va shaxsiy ma'lumotlar himoyasi kriptografiyaning ilmiy asoslangan, standartlarga mos va post-kvant xavflarni hisobga olgan holda rivojlantirilishiga bog'liq bo'ladi. Shu sababli mazkur sohada fundamental matematika, amaliy dasturlash, huquqiy tartibga solish va ta'lim tizimi o'zaro uyg'un rivojlanishi zarur.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi Prezidenti. "O'zbekiston Respublikasida kriptologiya sohasida ta'lim va ilm-fanni rivojlantirish chora-tadbirlari to'g'risida" PQ-293-son qaror. 15.08.2024.

2. O'zbekiston Respublikasi. "Kiberxavfsizlik to'g'risida" O'RQ-764-son Qonun. 15.04.2022.

3. O'zbekiston Respublikasi Prezidenti. "Raqamli O'zbekiston - 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida" PF-6079-son Farmon. 05.10.2020.

4. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.

5. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard. 2024.

6. National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Standard. 2024.

7. Diffie W., Hellman M. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976.

8. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978.

9. Koblitz N. Elliptic Curve Cryptosystems. Mathematics of Computation, 1987.

10. Miller V. Use of Elliptic Curves in Cryptography. Advances in Cryptology - CRYPTO, 1985.

11. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.

12. Buchmann J. Introduction to Cryptography. Springer, 2004.

13. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010.

14. Bernstein D. J., Lange T. Post-Quantum Cryptography. Nature, 2017.

15. Galbraith S. Mathematics of Public Key Cryptography. Cambridge University Press, 2012.

16. Smart N. P. Cryptography Made Simple. Springer, 2016.

17. Moldovyan A. A., Moldovyan N. A. Kriptografiya: teoriya i praktika. Sankt-Peterburg, 2002.

18. Sidelnikov V. M. Teoriya kodirovaniya i kriptografiya. Moskva, 2008.

19. Abdullayev R., Jo‘rayev A. Axborot xavfsizligi va kriptografik himoya asoslari. Toshkent, 2021.

20. ENISA. Post-Quantum Cryptography: Current State and Quantum Mitigation. European Union Agency for Cybersecurity, 2021.