KRIPTOGRAFIYADA SONLAR NAZARIYASINING ZAMONAVIY QO'LLANILISHI

Namangan davlat unversiteti Fizika-Matematika fakulteti matematika yo'nalishi 4-kurs talabasi
Suyumboyev Samandar Qodirjon o'g'li
samandarsuyumboyev24@gmail.com

Annotatsiya: *Mazkur maqolada sonlar nazariyasining kriptografiya sohasidagi ahamiyati, ayniqsa zamonaviy raqamli xavfsizlik tizimlarida uning o'rni yoritiladi. RSA va elliptik egri chiziqlar kriptografiyasi (ECC) kabi asosiy algoritmlarning matematik asoslari tahlil qilinadi. Shuningdek, katta sonlarni faktorizatsiya qilish muammosi, modul arifmetikasi, diskret logarifm masalasi kabi fundamental tushunchalarning kriptografik tizimlarda qo'llanishi ilmiy asosda bayon etiladi. Tadqiqot oxirida sonlar nazariyasining kelajakdagi qo'llanilish istiqbollari, jumladan kvant kriptografiyasi bilan bog'liq yo'nalishlar ko'rib chiqiladi.*

Kalit so'zlar: *kriptografiya, sonlar nazariyasi, RSA, ECC, modul arifmetikasi, xavfsizlik, diskret logarifm.*

KIRISH

Axborot texnologiyalari jadal rivojlanib borayotgan bugungi davrda ma'lumotlarni himoyalash masalasi dolzarb ahamiyat kasb etadi. Kriptografiya — bu ma'lumotlarni shifrlash va qaytarish jarayonini o'rganadigan fandir. Kriptografik tizimlarning katta qismi sonlar nazariyasi kabi matematikaning chuqur bo'limiga tayanadi. Katta tub sonlar, modul arifmetikasi, diskret logarifm masalasi, faktorizatsiya muammosi kabi masalalar zamonaviy xavfsizlik algoritmlarining asosiy tayanchidir. Hozirgi kunda Internet tarmoqlarida bank operatsiyalari, elektron to'lov tizimlari, shaxsiy muloqotlar, davlat axborot tizimlari aynan shu matematik tamoyillar asosida himoyalanadi. Shu sababli, sonlar nazariyasining kriptografiyada qo'llanilishi nafaqat nazariy, balki amaliy jihatdan ham juda muhimdir.

1. Sonlar nazariyasining kriptografiyadagi ahamiyati

Sonlar nazariyasi tub sonlar, ularning xossalari, modul bo'yicha arifmetika, kongruensiyalar, faktorizatsiya kabi tushunchalarni o'rganadi. Bu bo'limlar kriptografiyaning nazariy asoslari uchun poydevor vazifasini bajaradi.

1.1. Tub sonlarning roli

Ko'plab kriptografik algoritmlar, xususan RSA, ikki katta tub son ko'paytmasidan iborat modulga asoslanadi. Masalan, 1024–4096 bitlik tub

sonlar tanlab olinadi va ularni bir necha milliard yillarda ham faktorizatsiya qilish mumkin emas. Bu esa tizimning ishonchliligini ta’minlaydi.

1.2. Modul arifmetikasi

Modul bo‘yicha arifmetika Fermatning kichik teoremasi, Eyler funksiyasi, modulli darajalash kabi jarayonlar uchun keng qo‘llanadi. Kriptografiyada aynan ushbu arifmetika tez ishlashi va hisoblash murakkabligi bilan qadrlanadi.

1.3. Katta sonlarni faktorizatsiya qilish murakkabligi

Bugungi kunda eng yaxshi faktorizatsiya algoritmlari ham juda katta sonlarni bo‘lishni amalda imkonsiz qiladi. Kriptografiya aynan shu "murakkablik" ustiga qurilgan.

2. RSA algoritmining matematik asoslari

RSA — eng mashhur ochiq kalitli kriptografiya tizimidir. 1977-yilda Rivest, Shamir va Adleman tomonidan ishlab chiqilgan.

2.1. Asosiy g‘oya

Algoritm ikki katta tub sonni tanlashga asoslanadi:

- p va q — katta tub sonlar
- n=pq — modul
- φ(n)=(p−1)(q−1)

2.2. Ochiq va yopiq kalitlar

Ochiq kalit:

(e,n)

Yopiq kalit:

(d,n)

Bu yerda:

ed≡1 mod φ(n)

2.3. Shifrlash jarayoni

$C=Me \bmod n$

2.4. Deshifrlash jarayoni

$M=Cd \bmod n$

2.5. RSA xavfsizligi

RSA xavfsizligi katta sonni faktorizatsiya qilishning murakkabligiga tayanadi. Hozircha 2048 bitli sonni faktorizatsiya qilishga imkon beradigan real algoritm yo‘q.

3. Elliptik egri chiziqlar kriptografiyasi (ECC)

ECC — RSA ga nisbatan ko‘proq xavfsizlikni ta’minlaydigan zamonaviy kriptografiya usuli.

3.1. ECC ning matematik modeli

Elliptik egri quyidagi ko‘rinishda beriladi:

y2=x3+ax+b

Bunda egri ustida "nuqtalar guruhi" tashkil topadi va ular qo‘shish amali orqali yopiq sistemani hosil qiladi.

3.2. Diskret logarifm muammosi

ECC ning xavfsizligi elliptik egri diskret logarifm muammosi (ECDLP) ga asoslanadi. Bu masalani kompyuterlar amalda yecha olmaydi. Shu sababli ECC 256-bit kalit bilan RSA ning 3072-bit kalitiga teng xavfsizlik beradi.

3.3. Afzalliklari

Kalitlar kichik (256–384 bit),Tez ishlaydi, Mobil va IoT qurilmalar uchun eng qulay tizim

4. Zamonaviy kriptosistemalarda sonlar nazariyasining qo‘llanilishi

4.1. Blockchain va kriptovalyutalarda

Bitcoin, Ethereum kabi blokcheyn tizimlarida:

ECDSA (elliptik egri chiziqlar raqamli imzo algoritmi),hash funksiyalar, modulli arifmetika keng qo‘llanadi.

4.2. Raqamli imzo tizimlari

Raqamli imzo algoritmlari sonlar nazariyasi yordamida xabar muallifini tasdiqlash uchun ishlatiladi.

4.3. Internet xavfsizligi (TLS/SSL)

HTTPS protokoli aynan RSA, DH, ECC kabi usullarga tayanadi.

5. Kvant kompyuterlari va sonlar nazariyasi

Kvant kompyuterlar rivoji RSA algoritmiga xavf tug‘diradi, chunki Shor algoritmi katta sonlarni faktorizatsiya qilishni "tezlashtiradi". Shu sababli kvantga qarshi kriptografiya (Post-Quantum Cryptography) yo‘nalishi jadal rivojlanmoqda.

Sonlar nazariyasi yangi algoritmlarni ishlab chiqishda ham asosiy rol o‘ynamoqda.

XULOSA

Sonlar nazariyasi zamonaviy kriptografiya tizimlarining markazida turadi. RSA, ECC, blockchain, Internet xavfsizligi kabi ko‘plab texnologiyalar aynan tub sonlar, modul arifmetikasi, diskret logarifm muammosi kabi matematik tamoyillarga tayangan holda ishlaydi. Raqamli xavfsizlikning mustahkamligi sonlar nazariyasidagi ayrim muammolarni yechishning amaldagi imkonsizligi bilan bog‘liq. Kelajakda, xususan kvant kompyuterlar paydo bo‘lishi bilan ushbu sohada yangi matematik yondashuvlar talab etiladi.

FOYDALANILGAN ADABIYOTLAR:

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

2.Koblitz, N. (1987). Elliptic Curve Cryptosystems. Mathematics of Computation.

3.William Stallings. Cryptography and Network Security. Pearson Education.

4.Hoffstein, J., Pipher, J., Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.

5.Menezes, A. J., Van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography.

6.Katz, J., & Lindell, Y. (2015). Introduction to Modern Cryptography. CRC Press.

7.Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography.

8.NIST Post-Quantum Cryptography Project Reports.