ISSN 3060-4567

DISKRET LOGARIFMLASH ALGORITMI

Farg'ona davlat universiteti axborot
texnologiyalari kafedrasi mudiri
sa.rozaliyev@pf.fdu.uz
Ro'zaliyev Sherzodjon Avazjonovich
Farg'ona davlat universiteti 4-kurs talabasi
mamurovaroxatoy79@gmail.com
Alixo'jayeva Rohatoy Ilhomjon qizi

Annotatsiya:*Ushbu tezisda diskret logarifmlash algoritmi va uning kriptografiyada qo'llanilishi ko'rib chiqiladi. Diskret logarifmlash muammosi xavfsizlik asosida ishlaydigan ko'plab shifrlash tizimlarining poydevori hisoblanadi. Tezisda algoritm ishlash prinsiplari, samaradorligi va xavfsizlik jihatlari tahlil qilinadi.*

Kalit so'zlar: *diskret logarifm, kriptografiya, xavfsizlik, shifrlash algoritmi.*

Аннотация:*В данной работе рассматривается алгоритм дискретного логарифмирования и его применение в криптографии. Проблема дискретного логарифма является основой многих систем шифрования, основанных на безопасности. В работе анализируются принципы работы алгоритма, его эффективность и вопросы безопасности.*

Ключевые слова: *дискретный логарифм, криптография, безопасность, алгоритм шифрования.*

Annotation:*This thesis examines the discrete logarithm algorithm and its application in cryptography. The discrete logarithm problem forms the basis of many security-based encryption systems. The thesis analyzes the algorithm's operation principles, efficiency, and security aspects.*

Keywords: *discrete logarithm, cryptography, security, encryption algorithm.*

Diskret logarifm (Discrete Logarithm Problem — DLP) zamonaviy kriptografiyaning asosiy matematik tayanchlaridan biridir. DLP ko'plab xavfsizlik

ISSN 3060-4567

protokollarida — Diffie–Hellman kalit almashinuvida, ElGamal shifrlash tizimida, raqamli imzo algoritmlarida va elliptik egri chiziqli kriptografiyada muhim rol o'ynaydi.

Diskret logarifm quyidagi ko'rinishdagi masaladir:

Agar berilgan bo'lsa:

- p — tub son,
- g — $\mathbb{Z}_p^*$ guruhining generatori,
- $h = g^x \mod p$,

u holda **x ni topish masalasi diskret logarifm masalasi** deb ataladi:

$$x = \log_g h \quad (\mod p)$$

Bu masalani oddiy logarifmga o'xshash tarzda yechib bo'lmaydi, chunki amal diskret (modulyar) guruhda bajariladi. DLP aynan shu "teskari yo'nalish"ning murakkabligi bilan mashhur.

Diskret logarifm masalasining axborot xavfsizligidagi o'rni:

Diskret logarifmning yechilishi:

- kalit almashinuvi,
- shifrlash,
- raqamli imzolar,
- autentifikatsiya,

kabi kriptografik amallarga to'g'ridan-to'g'ri ta'sir qiladi.

Yirik kriptotizimlar DLPning amalda yechilmasligiga suyanadi.

Diskret logarifm masalasi (Discrete Logarithm Problem — DLP) axborot xavfsizligida asosiy matematik poydevorlardan biri bo'lib, ko'plab zamonaviy kriptografik tizimlarning xavfsizligi aynan bu masalaning murakkabligiga tayanadi.

1. DLP — Kriptografiyaning xavfsizlik asoslaridan biri

Diskret logarifm masalasini yechish juda qiyin (katta sonlarda), lekin modul bo'yicha daraja olish (g^x mod p) juda oson.Bu xususiyat *bir tomonlama funksiyalar*ni yaratadi, ya'ni:

- Hisoblash oson
- Teskari hisoblash qiyin

ISSN 3060-4567

Axborot xavfsizligi birinchi navbatda mana shunday funksiyalarga tayanadi.

2. Diskret logarifm asosidagi protokollar

Diffie–Hellman kalit almashinuvi-Ikkita foydalanuvchi maxfiy kalitni ochiq kanalda almashinmay turib olishi mumkin.Xavfsizligi DLP yechib bo'lmasligiga asoslanadi.

ElGamal shifrlash algoritmi-Davlat sektorida va ochiq standartlarda keng qo'llaniladi.Shifrlashning xavfsizligi **diskret logarifmni yechish qiyinligi**ga tayanadi.

DSA (Digital Signature Algorithm)-AQSH milliy raqamli imzo standarti.Imzo tekshirish jarayoni ham DLP yechilmasligiga asoslangan.

Elliptic Curve Cryptography (ECC – ECDLP)-Elliptik egri chiziqlardagi diskret log masalasi yanada qiyin.Shuning uchun ECC kichik kalitlar bilan ham yuqori xavfsizlik beradi.

3. DLP — Axborot xavfsizligining asosiy himoya tamoyillari

Diskret logarifm masalasi quyidagi xavfsizlik xususiyatlarini ta'minlaydi:

Konfidentsiallik (maxfiylik)-ElGamal yoki ECC shifrlash orqali ma'lumot tashqi shaxslardan yashiriladi.

Autentifikatsiya-DSA va ECDSA raqamli imzolar yordamida foydalanuvchining haqiqiyligini tasdiqlash mumkin.

Butunlik-Imzolar o'zgartirilmagan xabarni isbotlaydi.

Kalit almashishning xavfsizligi-Diffie–Hellman tufayli ikkita tomon xavfsiz kanalsiz maxfiy kalit oladi.

4. Agar diskret logarifm masalasi yechilsa nima bo'ladi?

Agar kimdir DLP ni juda tez yecha olsa:

- Diffie–Hellman buziladi
- ElGamal buziladi
- DSA va ECDSA imzolari qalbakilashtiriladi
- ECC asosidagi hamma protokollar xavf ostida qoladi

Shu sababli kriptografiya katta tub sonlar yoki murakkab elliptik egri chiziqlardan foydalanadi.

ISSN 3060-4567

5. Nima uchun DLP hal qilinmay qolmoqda?

Sabab:

- Modul $p \geq 2048$ bit bo'lsa, eng tez algoritmlar ham amalda juda sekin
- Index calculus / Number field sieve usullari ham juda katta p uchun ishlamaydi
- Elliptik egri chiziqlarda esa hatto 256-bit ham yetarli xavfsizlik beradi

Shuning uchun diskret logarifm masalasi kriptoxavfsizlikning mustahkam poydevori bo'lib turibdi.

Diskret logarifmni yechish algoritmlari: umumiy tasnif

Algoritmlar ikkiga bo'linadi:

1) Ekspotensial murakkablikdagi usullar

→ kichik sonlar uchun ishlaydi

2) Sub-ekspotensial algoritmlar

→ katta modullar uchun eng tezkor (lekin hali ham amaliy yechim emas)

Elliptik egri chiziqli diskret logarifm (ECDLP):Elliptik egri chiziqlarda yuqoridagi algoritmlarning **deyarli hech biri ishlamaydi.**

ECDLPni yechish uchun amalda:

1) Pollard's Rho for ECC

- Murakkablik **O(√n)**
- ECC xavfsizligini belgilaydi

2) BSGS (nazariy)

- Xotira juda ko'p talab qiladi

Muhim natija: Ko'plab algoritmlar ECC guruh tuzilmasida ishlamagani uchun elliptik egri chiziqli kriptografiya juda kuchli hisoblanadi.

DLP xavfsizligi va kriptografiyada qo'llanilishi:

Diskret logarifm quyidagi tizimlarning xavfsizligini belgilaydi:

- Diffie–Hellman kalit almashinuvi
- ElGamal shifrlash tizimi
- DSA (Raqamli imzo)
- ECDH va ECDSA (elliptik egri chiziqli algoritmlar)

ISSN 3060-4567

Asosiy xavfsizlik mezoni: Modul yoki guruh shunchalik katta bo'lishi kerakki, mavjud eng tezkor algoritmlar ham amalda uni yecha olmasin.

Algoritmlarni taqqoslash:

Algoritm	Murakkablik	Xotira	Izoh
Brute Force	O(p)	kam	Faqat kichik p
BSGS	O(√p)	√p	Deterministik
Pollard Rho	O(√p)	juda kam	Amaliyda yaxshi
Pohlig–Hellman	faktorlarga bog'liq	o'rta	p−1 "yomon" bo'lsa oson
Index Calculus	$L_p[1/2]$	katta	Katta p uchun

Xulosa:

Diskret logarifmlash algoritmi kriptografiyada muhim o'rin tutadi va xavfsiz shifrlash tizimlarining poydevori hisoblanadi. Ushbu tezisda algoritmning matematik asoslari, ishlash samaradorligi va zamonaviy kripto tizimlaridagi qo'llanilishi tahlil qilindi. Tadqiqot shuni ko'rsatdiki, diskret logarifmga asoslangan tizimlar, ayniqsa, katta modul va quvvatli algoritmlar yordamida yuqori darajadagi xavfsizlikni ta'minlaydi. Shu bilan birga, samarali hisoblash usullarini qo'llash orqali amaliy ishlatish qulayligi oshiriladi.Diskret logarifm masalasi axborot xavfsizligi nazariyasida markaziy o'rinni egallaydi. Ushbu masalaning qiyin yechilishi ko'plab kriptotizimlarning mustahkamligi uchun asos bo'ladi. DLPni yechishga mo'ljallangan algoritmlar matematika, chiziqli algebra, ehtimollar nazariyasi va sonlar nazariyasining chuqur yutuqlariga tayangan bo'lsa ham, yirik parametrli zamonaviy tizimlar uchun ular amaliy tarzda samarali emas.Shu sababli kriptografiya amaliyotida **katta darajadagi tub sonlar, elliptik egri chiziqlar, rezistent guruhlar** kabi yechimlar qo'llanilmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Koblitz, N. (1994). *A Course in Number Theory and Cryptography*. Springer.
2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*. CRC Press.

ISSN 3060-4567

3. Silverman, J. H. (2009). *An Introduction to Mathematical Cryptography*. Springer.

4. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.

5. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

6. Boneh, D., & Shoup, V. (2020). *A Graduate Course in Applied Cryptography*. Version 0.5.