GCCR
Global Conference on Contemporary Research

GLOBAL CONFERENCE ON CONTEMPORARY RESEARCH



CONFERENCE THEME:

SUSTAINABLE FUTURES:
INNOVATION, DIGITAL TRANSFORMATION AND GLOBAL COLLABORATION THROUGH CONTEMPORARY RESEARCH

INNOVATION | DIGITAL TRANSFORMATION | GLOBAL COLLABORATION | SUSTAINABLE FUTURES

JOURNAL

PEER-REVIEWED PROCEEDINGS

OCTOBER 2026

TORONTO, CANADA

gccr.academy

APPLICATIONS OF COMPARISON THEORY IN MODERN INFORMATION SECURITY AND CRYPTOGRAPHY

Qurbonov Shuhrat Yo'ldoshevich
Second-Year Master's student
Termez State Pedagogical Institute
https://doi.org/10.5281/zenodo.23796084

KIRISH: AXBOROT XAVFSIZLIGI DAVRI. Hozirgi globallashgan va to'liq raqamlashtirilgan axborot texnologiyalari asrida har soniyada milliardlab ma'lumotlar global tarmoqlar orqali uzatiladi. Bank tranzaksiyalari, davlat sirlari, shaxsiy ma'lumotlar va korporativ yozishmalarning xavfsizligini kafolatlash zamonaviy ilm-fanning eng muhim strategik vazifalaridan biriga aylangan.

Ushbu raqamli himoya tizimlarining markazida esa asrlar oldin yaratilgan va faqat sof (mavhum) matematikaga tegishli deb hisoblangan nazariyalar, xususan, sonlar nazariyasi va uning taqqoslamalar (congruences) bo'limi yotadi.

Bir qarashda oddiy munosabatdek ko'rinadigan $a \equiv b \pmod{m}$ taqqoslamasi bugungi kunda internetdagi barcha xavfsiz ulanishlarni (HTTPS, SSL/TLS protokollari), raqamli imzolarni va elektron to'lovlarni himoya qiluvchi kuchli qalqon vazifasini bajarmoqda. Ushbu tezisda taqqoslamalar nazariyasining zamonaviy kriptografiyadagi bevosita tatbiqlari hamda ularning ishlash prinsiplari mufassal tahlil etiladi.

KRIPTOGRAFIYA VA MODULLI ARIFMETIKA UZVIY BOG'LIQLIGI. Kriptografiya fani asosan ikki katta yo'nalishga bo'linadi: simmetrik shifrlash (bunda shifrlash va deshifrlash uchun bitta umumiy kalit ishlatiladi) va asimmetrik shifrlash (ochiq va yopiq kalitlar tizimi). Taqqoslamalar nazariyasi asimmetrik shifrlashning yuzaga kelishida revolyutsion o'rin tutdi.

Klassik kriptografiyada murakkablik asosan aralashtirish va almashtirish kabi lingvistik amallarga asoslangan bo'lsa, zamonaviy axborot xavfsizligi o'z poydevorini kompyuterlar uchun yechilishi asrlar talab qiladigan murakkab matematik muammolarga qurgandir.

Modulli arifmetikaning o'ziga xos xususiyati shundaki, u chekli maydonlarda yoki halqalarda hisoblash olib boradi. Bu xususiyat jarayonni oldinga qarab hisoblashni oson, lekin orqaga qarab (teskari funksiya orqali) hisoblashni esa o'ta mashaqqatli qiladi. Masalan, x ≡ g^a (mod p) ifodada g, a, va p ma'lum bo'lsa x ni topish juda onson (modulli darajaga ko'tarish). Biroq x, g va p ma'lum bo'lganda, daraja ko'rsatkichi 'a' ni topish masalasi 'Diskret logarifm muammosi' deb ataladi va uning samarali algoritmik yechimi hozirgacha mavjud emas.

RSA ALGORITMI - TAQQOSLAMALARNING TANTANASI. Zamonaviy kriptografiyaning tayanch ustunlaridan biri bo'lgan RSA (Rivest, Shamir, Adleman) ochiq kalitli shifrlash tizimi to'g'ridan-to'g'ri Eyler teoremasi va modulli arifmetikaga asoslanadi. Bu algoritm p va q kabi ikkita juda katta (yuzlab raqamlardan iborat) tub sonlarni ko'paytirishning onsonligi, ammo hosil bo'lgan ko'paytmani yana qaytadan ikkita tub songa ajratishning (faktoring muammosi) texnik jihatdan ilojsizligi g'oyasiga qurilgan.

RSA algoritmi uch bosqichda amalga oshiriladi. Birinchi bosqichda foydalanuvchi ikkita ulkan p va q tub sonlarini tanlaydi va ularning ko'paytmasi n = p*q modulni hisoblaydi. So'ngra Eyler funksiyasi orqali phi(n) = (p-1)*(q-1) topiladi.

Ikkinchi bosqichda e ochiq kalit phi(n) bilan o'zaro tub qilib olinadi. Yopiq kalit d esa e*d ≡ 1 (mod phi(n)) taqqoslamasini yechish orqali (Kengaytirilgan Yevklid algoritmi yordamida) topiladi.

Ma'lumotni (M) shifrlash jarayoni (C) aynan modulli darajaga ko'tarish amali orqali bajariladi: C ≡ M^e (mod n). Hujjatni deshifrlash uchun yopiq kalit egasi C^d ≡ (M^e)^d ≡ M (mod n) amalini bajaradi. Ushbu formulaning to'g'riligi Eyler teoremasining bevosita isbotiga tayanadi.

DIFFI-XELMAN PROTOKOLI VA RAQAMLI IMZOLAR. Axborot xavfsizligidagi yana bir eng muhim ixtirolardan biri Diffi-Xelman (Diffie-Hellman) kalit almashish protokolining kashf etilishidir. Ochiq kanallar (masalan, internet) orqali aloqa qilayotgan ikki tomon xavfsiz yashirin kalitga kelishib olishlari kerak bo'ladi. Diffi-Xelman

usuli tub modul p bo'yicha ibtidoiy ildizlarning xossalariga va taqqoslamalarga tayanadi.

Har bir qatnashchi o'zining yashirin x sonini tanlaydi va y ≡ g^x (mod p) qiymatni ochiq tarmoqqa yuboradi. Boshqa qatnashchi qabul qilib olgan qiymatni o'zining yashirin soni darajasiga ko'taradi. Modulli arifmetikaning (g^x)^y ≡ (g^y)^x (mod p) ajoyib xossasi tufayli ikkala tomon ham tashqaridan kuzatuvchiga noma'lum bo'lgan bir xil sirli kalitga ega bo'lishadi.

Hujjatlarning haqiqiyligini va o'zgartirilmaganligini kafolatlovchi raqamli imzolar tizimi (Digital Signatures) ham taqqoslamalarga asoslangan. Xabarning hesji (hash qiymati) yopiq kalit orqali shifrlanib yuboriladi. Qabul qiluvchi esa ochiq kalit yordamida modul qoldig'ini tekshirib (taqqoslab) muallifning haqiqiyligini tasdiqlaydi.

XITOY QOLDIQLAR TEOREMASINING KRIPTOGRAFIYADAGI O'RNI. Axborot texnologiyalari rivojlanib, shifrlash kalitlarining uzunligi (2048, 4096 bit) oshib borgani sari kompyuterlarning protsessoriga tushadigan yuklama ham ortib bordi. Katta sonlar ustida taqqoslama (modul) hisoblashlarini tezlashtirish matematik optimallashtirishni talab qildi.

Aynan shu yerda Xitoy qoldiqlar teoremasi (XQT) yordamga keldi. RSA algoritmini deshifrlash jarayonida C^d (mod n) ifodasini to'g'ridan-to'g'ri hisoblash o'rniga, n = p*q bo'lgani uchun, hisoblashlar C^d (mod p) va C^d (mod q) ko'rinishidagi ikkita kichikroq ifodalarga ajratiladi. Kichik modullardagi hisoblash natijalari so'ngra XQT yordamida qayta birlashtirilib, yakuniy natija olinadi.

Bu usul (RSA-CRT) deshifrlash jarayonini deyarli to'rt barobarga tezlashtiradi va hozirgi kundagi barcha smartfonlar va serverlarda standart hisoblash metodi sifatida ishlatiladi.

XULOSA. Xulosa o'rnida shuni chuqur ta'kidlash lozimki, Gauss, Ferma va Eyler kabi buyuk matematiklar tomonidan qirrasi taralgan taqqoslamalar nazariyasi bugungi raqamli va axborotlashgan jamiyatda o'zining haqiqiy beqiyos amaliy tatbiqini topdi.

U nafaqat matematik teoremani isbotlash vositasi, balki global elektron tijorat,

kiberxavfsizlik, raqamli valyutalar (blokcheyn) va axborot himoyasi kabi sohalarning asabiy tomirlarini saqlab turuvchi ajralmas tizimga aylanib ulgurdi. Taqqoslamalar nazariyasisiz biz bilgan zamonaviy, xavfsiz va tezkor internet olami umuman mavjud bo'lmagan bo'lar edi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed. Pearson, 2017.
2. Rivest R. L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126, 1978.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. John Wiley & Sons, 1996.
4. Koblitz N. A Course in Number Theory and Cryptography. Springer, 1994.
5. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996.