ZAMONAVIY KRIPTOGRAFIYANING MATEMATIK ASOSLARI VA AMALIY QO'LLANILISHI

Jo'raqulova Munisa O'ktam qizi

Mirzo Ulug'bek Nomidagi O'zbekiston Milliy Universiteti

Amaliy Matematika Fakulteti 4-bosqich talabasi

ANNOTATSIYA: Internet xavfsizligi va ma'lumotlarni himoya qilish barcha foydalanuvchilar uchun kafolatlangan bo'lishi kerak. Shu sababli, ma'lumotlarni tarmoqlarda tarqatishda xavfsizlik muhim masalalardan biridir. Bugungi kunda ma'lumotlar hech qachon kerakli darajada himoyalanmaydi. Kriptografiya esa tarmoq xavfsizligining eng samarali va ishonchli tarkibiy qismlaridan biridir. Kriptografiya – bu yuboruvchi va qabul qiluvchi o'rtasida tushunarsiz shaklda uzatiladigan ma'lumotlarni ishonchli va xavfsiz tarzda almashinishni ta'minlovchi usuldir. Bundan tashqari, faqat ruxsat etilgan qabul qiluvchi yuboruvchi tomonidan shifrlangan ma'lumotni qayta tiklash (deshifrlash) huquqiga ega bo'ladi. Kriptografiya tarmoqlarga xavfsizlikni ta'minlashda muhim rol o'ynaydi. Ushbu maqolada biz turli algoritmlarning tasodifiy hajmdagi ma'lumot paketlarida shifrlash va deshifrlash vaqtini kuzatamiz. Avvalo, ushbu ishda kriptografiyaning asosiy tushunchalari – shifrlash va deshifrlash amallari kiritiladi. Keyin esa eng mashhur algoritmlar – RSA, El-Gamal va Elliptik Egri (ECC) o'rtasidagi taqqoslash ko'rib chiqiladi. [1].

KALIT SO'ZLAR: Kriptografiya, RSA algoritmi ,kvant kompyuterlar,sonlar nazariyasi, post-kvant kriptografiya.

KIRISH: Axborot xavfsizligi bugungi kunda global muammo sifatida qaralmoqda. Internet, moliya, davlat boshqaruvi va shaxsiy ma'lumotlar almashinuvida axborotning maxfiyligi, butunligi va ishonchliligini ta'minlash uchun samarali matematik yondashuvlar zarur. Shu nuqtai nazardan, kriptografiya fani nafaqat matematik nazariyaga, balki amaliyotga ham tayanadi. Ayniqsa, sonlar nazariyasining tub sonlar, modul arifmetikasi va diskret logarifm kabi tushunchalari zamonaviy kriptotizimlarning asosi hisoblanadi [2].

ASOSIY QISM

Kriptografiyaning nazariy asoslari: Kriptografiyada sonlar nazariyasi eng asosiy manba bo‘lib xizmat qiladi. Masalan, RSA algoritmi tub sonlar va modul arifmetikasiga asoslanadi. RSA xavfsizligi katta sonlarni faktorizatsiya qilishning murakkabligiga tayanadi [3]. Shuningdek, diskret logarifm masalasi ham ko‘plab shifrlash usullarida qo‘llaniladi.

Asosiy kriptografik algoritmlar- RSA – 1977 yilda ishlab chiqilgan bo‘lib, sonlar nazariyasining eng mashhur qo‘llanilishidir. Uning xavfsizligi katta tub sonlarni ko‘paytirish oson, ammo ajratib yozish (faktorizatsiya qilish) juda qiyinligiga asoslanadi. Elliptik egri chiziqlar kriptografiyasi (ECC) – bu usul kichikroq kalit uzunligida yuqori xavfsizlikni ta’minlaydi. ECC kriptografiyasi hozirgi zamon mobil qurilmalarida keng qo‘llanilmoqda [4].Zamonaviy muammolar va istiqbollar: Kvant kompyuterlar rivojlanishi bilan hozirgi shifrlash usullarining barqarorligi savol ostida qolmoqda. Kvant hisoblash asosida faktorizatsiya yoki diskret logarifmni yechish ancha osonlashishi mumkin. Shu sababli, post-kvant kriptografiya yo‘nalishlari faol rivojlanmoqda [5].

Baholash parametrlari: Har bir shifrlash texnikasining o‘ziga xos kuchli va zaif tomonlari mavjud. Ma’lum bir ilovaga mos kriptografiya algoritmini qo‘llash uchun uning ishlash samaradorligi, kuchli va zaif tomonlari haqida ma’lumotga ega bo‘lishimiz kerak. Shuning uchun ushbu algoritmlar bir nechta xususiyatlarga asoslanib tahlil qilinishi lozim. Ushbu maqolada kriptotizimlarni taqqoslash uchun quyidagi mezonlar asosida tahlil amalga oshiriladi:

Shifrlash vaqti: Oddiy matnni shifr-matnga aylantirish uchun ketgan vaqt shifrlash vaqti deyiladi. Shifrlash vaqti kalit hajmiga, oddiy matn blokining hajmiga va rejimga bog‘liq. Bizning tajribamizda shifrlash vaqti millisekundlarda o‘lchangan. Shifrlash vaqti tizim unumdorligiga ta’sir qiladi. Shifrlash vaqti imkon qadar qisqa bo‘lishi kerak, bu esa tizimni tez va samarali qiladi.

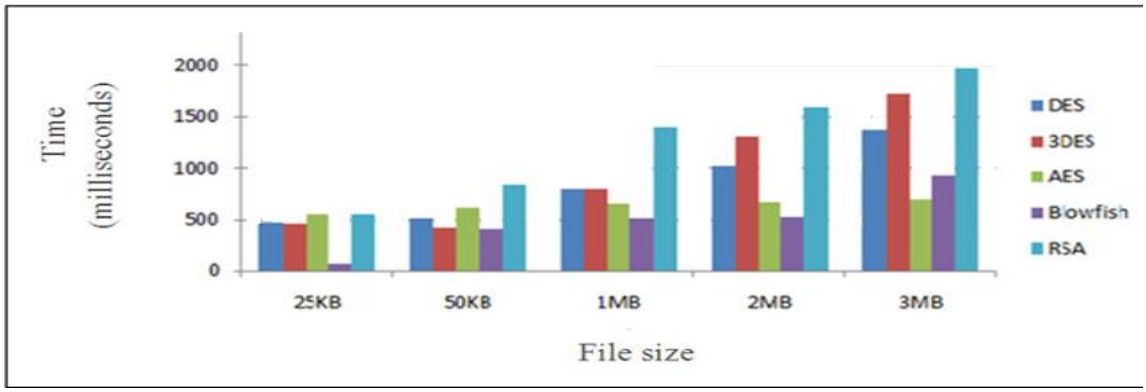
Deshifrlash vaqti: Shifr-matndan oddiy matnni tiklash uchun ketgan vaqt deshifrlash vaqti deyiladi. Deshifrlash vaqti ham xuddi shifrlash vaqtiga o‘xshash tarzda qisqa bo‘lishi

kerak, shunda tizim tez va samarali ishlaydi. Deshifrlash vaqti tizim unumdorligiga ta’sir qiladi. Bizning tajribamizda deshifrlash vaqti ham millisekundlarda o‘lchangan.

“Avalanche” effekti: Kriptografiyada **diffuziya** deb ataluvchi xususiyat algoritmning kriptografik kuchini aks ettiradi. Agar kirishda kichik o‘zgarish bo‘lsa, chiqishda katta o‘zgarish yuz beradi. Bu “avalanche” effekti deb ataladi. Biz “avalanche” effektini **Hamming masofasi** yordamida o‘lchadik. Axborot nazariyasida Hamming masofasi o‘xshamaslik darajasini ko‘rsatadi. Biz uni bitma-bit XOR orqali ASCII qiymatlarini hisoblab topdik, chunki bu dasturiy jihatdan oson amalga oshiriladi. Diffuziya darajasi qanchalik yuqori bo‘lsa, ya’ni “avalanche” effekti kuchli bo‘lsa, shunchalik yaxshi. “Avalanche” effekti kriptografik algoritmning samaradorligini aks ettiradi.

$$Avalanche\ effecti = \frac{Hamming\ masofasi}{fayl\ hajmi}$$

Shifrlash vaqti:



1-rasm. DES, 3DES, AES, Blowfish va RSA algoritmlari uchun shifrlash vaqti va fayl hajmi taqqoslanishi.

1-rasmda ko‘rsatilganidek, 3DES – bu DES algoritmini uch marta turli kalitlar bilan ketma-ket qo‘llash orqali yaratilgan. U dastlab xavfsiz hisoblangan bo‘lsa-da, dasturiy ta’minotda samarali emas. RSA esa shifrlash uchun eng ko‘p vaqt talab qiladi. Blowfish esa barcha algoritmlar ichida eng kam vaqtni sarflaydi. Blowfish kalitga bog‘liq qidiruv jadvallaridan foydalanadi; shuning uchun uning unumdorligi platformaning xotira va

keshni qay darajada samarali boshqarishiga bog‘liq. Shunday bo‘lsada, Blowfish dasturiy jihatdan samarali va tez ishlaydi[6].

XULOSA

Kriptografiya va sonlar nazariyasi zamonaviy xavfsizlik tizimlarining poydevorini tashkil etadi. RSA va ECC kabi algoritmlar bugungi kunda keng qo‘llanilmoqda, biroq kvant texnologiyalari rivojlanishi ularning barqarorligini shubha ostiga qo‘ymoqda. Shu boisdan, post-kvant kriptografiya yo‘nalishida yangi matematik usullarni ishlab chiqish zarur. O‘zbekistonning ham kriptografik yechimlarni huquqiy asosda tartibga solishga e’tibor qaratayotgani bu sohada muhim qadamdir.

FOYDALANILGAN ADABIYOTLAR

1.A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms | IEEE Conference Publication | IEEE Xplore

2. Katz, J., & Lindell, Y. (2015). Introduction to Modern Cryptography. PDF.

3. Goldwasser, S. (2002). Mathematical foundations of modern cryptography: computational complexity perspective. arXiv:cs/0212055.

4. Galbraith, S. (2005). Algebraic curves and cryptography. Journal of Computational and Applied Mathematics. ScienceDirect.

5. Arxiv (2018). The Impact of Quantum Computing on Present Cryptography. arXiv:1804.00200.

6. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish - ScienceDirect.