ISSN 3060-4567

AXBOROTLARNI SHIFRLASHDA MATEMATIK ALGORITMLARDAN FOYDALANISH

Farmonov Sherzodbek Raxmonjonovich
Farg'ona davlat universiteti amaliy matematika va informatika kafedrasi katta o'qituvchisi
farmonovsh@gmail.com
Solijonova Gulsanam Sodirjon qizi
Farg'ona davlat universiteti talabasi
gulsanamsolijonova18@gmail.com

Annotatsiya: *Axborotlarni shifrlashda matematik algoritmlar zamonaviy axborot xavfsizligining asosini tashkil etadi. Ushbu algoritmlar ma'lumotlarni maxfiy va himoyalangan holatda saqlash uchun murakkab matematik usullardan foydalanadi. Simmetrik shifrlash algoritmlari (masalan, AES va DES) tezkorligi bilan ajralib turib, asosan, modulyar arifmetika va XOR operatsiyalariga tayanadi. Assimetrik shifrlash algoritmlari (masalan, RSA va ElGamal) esa ochiq va yopiq kalitlardan foydalanib, katta tub sonlar va diskret logaritm masalasi kabi murakkab matematik tamoyillarga asoslanadi.*

Kalit so'zlar: *axborot xavfsizligi, shifrlash algoritmlari, simmetrik shifrlash, assimetrik shifrlash, RSA, AES, xesh funksiyalari, elliptik egri kriptografiya (ECC), matematik tamoyillar, tub sonlar, diskret logarithm, XOR operatsiyasi, modul arifmetikasi*

Annotatsiya: *Mathematical algorithms in information encryption form the foundation of modern information security. These algorithms utilize complex mathematical methods to keep data confidential and secure. Symmetric encryption algorithms (e.g., AES and DES) are known for their speed and rely on modular arithmetic and XOR operations. Asymmetric encryption algorithms (e.g., RSA and ElGamal) use public and private keys, based on principles like large prime numbers and the discrete logarithm problem.*

ISSN 3060-4567

Keywords: *Information security,encryption algorithms, symmetric encryption, asymmetric encryption, RSA, AES, hash functions, elliptic Curve Cryptography (ECC), mathematical principles, prime numbers, discrete logarithm, XOR operation, modular arithmetic*

Аннотация: *Математические алгоритмы в шифровании информации являются основой современной информационной безопасности. Эти алгоритмы используют сложные математические методы для обеспечения конфиденциальности и защиты данных. Симметричные алгоритмы шифрования (например, AES и DES) известны своей скоростью и базируются на модульной арифметике и операциях XOR. Асимметричные алгоритмы шифрования (например, RSA и ElGamal) используют открытые и закрытые ключи, основанные на таких принципах, как большие простые числа и задача дискретного логарифма.*

Ключевые слова: *Информационная безопасность, алгоритмы шифрования, симметричное шифрование, асимметричное шифрование, RSA, AES, хэш-функции, криптография на эллиптических кривых (ECC), математические принципы, простые числа, дискретный логарифм, операция XOR, модульная арифметика.*

Axborotlarni shifrlashda matematik algoritmlar axborot xavfsizligini ta'minlashda muhim rol o'ynaydi. Shifrlash algoritmlari axborotni maxfiylashtirish uchun murakkab matematik jarayonlardan foydalanadi. Bu algoritmlar axborotni tushunarsiz ko'rinishga keltiradi va faqat tegishli kalit yordamida uni o'qishga imkon beradi. Quyida shifrlash algoritmlarining asosiy turlari va ularning matematik asosi keltirilgan:

Simmetrik shifrlash algoritmlari

Simmetrik algoritmlar shifrlash va deshifrlash uchun bitta (bir xil) kalitdan foydalanadi. Eng mashhur simmetrik algoritmlar:

AES (Advanced Encryption Standard): Matritsa va polinom operatsiyalariga asoslangan. Masalan:

Galois maydonida (GF(2^8)) bo'lib, matritsa multiplikatsiyasi va almashtirish ishlatiladi.

DES (Data Encryption Standard): XOR operatsiyalari va permutationlardan foydalanadi.

Matematik tamoyillari:

Modulo arifmetikasi.

XOR operatsiyalari.

Matritsa va vektorlar algebrai.

Masala: Elliptik egri kriptografiyasidan foydalanib xabarni shifrlash va deshifrlash

Elliptik egri kriptografiyasi (ECC) yordamida xabarni shifrlang va deshifrlang.

Shartlar:

1. Elliptik egri tenglamasi berilgan:

y^2 = x^3 + 2x + 3 \, (\mod 97)

2. Jamoat kaliti uchun bazaviy nuqta () tanlangan:

G = (3, 6)

3. Foydalanuvchi A va B o‘zining maxfiy kalitlarini tanlaydi:

Foydalanuvchi A: (maxfiy kalit)

Foydalanuvchi B: (maxfiy kalit).

4. Xabarni kodlash uchun elliptik egri ustidagi nuqtalardan foydalaning.

Berilgan xabar: (xabar elliptik egrida aniqlangan nuqta ko‘rinishida berilgan).

C# Kod: Elliptik Egri Kriptografiyasi

```
using System;
using System.Numerics;
class ECC
{    // Elliptik egrining parametrlari
   static int a = 2; // Elliptik egri tenglamasi: y^2 = x^3 + ax + b (mod p)
   static int b = 3;
```

```
static int p = 97; // Modulus (prime number)
// Nuqtani qo'shish (Elliptik egrida)
static (BigInteger, BigInteger) AddPoints((BigInteger, BigInteger) P, (BigInteger, BigInteger) Q)
{       if (P == (0, 0)) return Q; // Agar P nol nuqta bo'lsa
   if (Q == (0, 0)) return P; // Agar Q nol nuqta bo'lsa
   if (P.Item1 == Q.Item1 && (P.Item2 + Q.Item2) % p == 0) return (0, 0); // Teskari nuqtalar
   BigInteger lambda;
   if (P != Q) // Oddiy qo'shish
   {           lambda = ((Q.Item2 - P.Item2) * ModInverse(Q.Item1 - P.Item1, p)) % p;
   }       else // Nuqtani ikki barobar oshirish
   {           lambda = ((3 * P.Item1 * P.Item1 + a) * ModInverse(2 * P.Item2, p)) % p;
   }       BigInteger x3 = (lambda * lambda - P.Item1 - Q.Item1) % p;
   BigInteger y3 = (lambda * (P.Item1 - x3) - P.Item2) % p;
   return ((x3 + p) % p, (y3 + p) % p); // Salbiy qiymatlarni oldini olish uchun    }    // Nuqtani ko'paytirish (Elliptik egrida)
static (BigInteger, BigInteger) MultiplyPoint((BigInteger, BigInteger) P, BigInteger k)
{       (BigInteger, BigInteger) R = (0, 0); // Nol nuqta
   (BigInteger, BigInteger) Q = P;
   while (k > 0)
   {           if ((k & 1) == 1)
         R = AddPoints(R, Q);
      Q = AddPoints(Q, Q);
      k >>= 1;
   }       return R;
}    // Modulyar teskari hisoblash (Euclid algoritmi asosida)
```

```
static BigInteger ModInverse(BigInteger k, BigInteger mod)
{       BigInteger m0 = mod, t, q;
   BigInteger x0 = 0, x1 = 1;
   if (mod == 1) return 0;
   while (k > 1)
   {          q = k / mod;          t = mod;          mod = k % mod;
      k = t;          t = x0;          x0 = x1 - q * x0;          x1 = t;       }
   if (x1 < 0)          x1 += m0;       return x1;    }
static void Main(string[] args)    {       // Bazaviy nuqta G       var G =
(3, 6);
   // Foydalanuvchilar maxfiy kalitlari
   BigInteger nA = 45; // Foydalanuvchi A
   BigInteger nB = 20; // Foydalanuvchi B
   // Jamoat kalitlarini hisoblash
   var PA = MultiplyPoint(G, nA);
   var PB = MultiplyPoint(G, nB);
   Console.WriteLine($"Foydalanuvchi A jamoat kaliti: ({PA.Item1},
{PA.Item2})");
   Console.WriteLine($"Foydalanuvchi B jamoat kaliti: ({PB.Item1},
{PB.Item2})");
   // Xabar (M) nuqtasi
   var M = (10, 22);
   // Shifrlash
   BigInteger k = 15; // Tasodifiy butun son
   var C1 = MultiplyPoint(G, k);
   var C2 = AddPoints(M, MultiplyPoint(PB, k));
   Console.WriteLine($"Shifrlangan    xabar:    C1    =    ({C1.Item1},
{C1.Item2}), C2 = ({C2.Item1}, {C2.Item2})");
   // Deshifrlash
   var M_decoded = AddPoints(C2, MultiplyPoint(C1, -nB));
```

Console.WriteLine($"Deshifrlangan xabar: ({M_decoded.Item1}, {M_decoded.Item2})");

}}Kodning ishlash prinsipi

1. Nuqtalarni qo'shish va ko'paytirish: Elliptik egri ustidagi operatsiyalar algoritmda modulyar arifmetika asosida amalga oshiriladi.

2. Shifrlash:

Xabar M tasodifiy yordamida kodlanadi va , juftliklari olinadi.

3. Deshifrlash:

orqali xabar qayta ochiladi.

4. Kod barcha bosqichlarni birgalikda hisoblaydi va natijalarni chop etadi.

Elliptik egri kriptografiyasi (ECC) — zamonaviy kriptografiya sohasidagi eng samarali va xavfsiz texnologiyalardan biri bo‘lib, u axborotlarni himoya qilishda yuqori darajadagi maxfiylikni ta’minlaydi. ECC kichik kalit o‘lchamlari bilan yuqori xavfsizlikni ta’minlash imkonini berib, resurslarni tejaydi va tarmoqdagi operatsiyalarni tezlashtiradi. Bu texnologiya, ayniqsa, cheklangan hisoblash quvvatiga ega bo‘lgan qurilmalarda (masalan, mobil telefonlar, IoT qurilmalari) keng qo‘llaniladi. Ushbu algoritmning matematik asosi — elliptik egri ustida ishlovchi nuqtalar va ularning modulyar arifmetikasi, bu esa deshifrlashni hisoblash jihatidan murakkab qiladi va axborot xavfsizligini oshiradi.

FOYDALANILGAN ADABIYOTLAR:

1.Н. А. Тюкачев, В. Г. Хлебостроев. C#. Алгоритмы и структуры данных: учебное пособие для СПО. – СПб.: Лань, 2021. – 232 с.

2. Mykel J. Kochenderfer. Tim A. Wheeler. Algorithms for Optimization. Published by The MIT Press., in London, England. 2019. – 500 p.

3. Рафгарден Тим. Совершенный алгоритм. Графовые алгоритмы и структуры данных. – СПб.: Питер, 2019. - 256 с.

https://scientific-jl.org/index.php/luch Часть-34_ Том-1_ Декабрь

4. Ахо Альфред В., Ульман Джеффри Д., Хопкрофт Джон Э. Структуры данных и алгоритмы. – М.: Вильямс, 2018. – 400 с.

5. Дж.Хайнеман, Г.Поллис, С.Стэнли. Алгоритмы. Справочник с примерами на C, C++, Java и Python, 2-е изд.: Пер. с англ. — СпБ.: ООО "Альфа-книга", 2017. — 432 с.

6. Farmonov, S., & Nazirov, A. (2023). C# DASTURLASH TILIDA GRAY KODI BILAN ISHLASH. B CENTRAL ASIAN JOURNAL OF EDUCATION AND INNOVATION (Т. 2, Выпуск 12, сс. 71–74). Zenodo.

7. Farmonov, S., & Toirov, S. (2023). NETDA DASTURLASHNING ZAMONAVIY TEXNOLOGIYALARINI O'RGANISH. *Theoretical aspects in the formation of pedagogical sciences*, *2*(22), 90-96

8. Raxmonjonovich, F. S. (2023). Array ma’lumotlar tizimini talabalarga o’qitishda Blockchain metodidan foydalanish. *Yangi O'zbekiston taraqqiyotida tadqiqotlarni o'rni va rivojlanish omillari*, *2*(2), 541-547.

9. Raxmonjonovich, F. S. (2023). Dasturlashda interfeyslardan foydalanishning ahamiyati. *Yangi O'zbekiston taraqqiyotida tadqiqotlarni o'rni va rivojlanish omillari*, *2*(2), 425-429.

10. Raxmonjonovich, F. S. (2023). Dasturlashda obyektga yo’naltirilgan dasturlashning ahamiyati. *Yangi O'zbekiston taraqqiyotida tadqiqotlarni o'rni va rivojlanish omillari*, *2*(2), 434-438.

11. Raxmonjonovich, F. S. (2023). Dasturlash tillarida fayllar bilan ishlash mavzusini Blended Learning metodi yordamida o'qitish. *Yangi O'zbekiston taraqqiyotida tadqiqotlarni o'rni va rivojlanish omillari*, *2*(2), 464-469.

12. Raxmonjonovich, F. S. (2023). DASTURLASHDA ISTISNOLARNING AHAMIYATI. *Yangi O'zbekiston taraqqiyotida tadqiqotlarni o'rni va rivojlanish omillari*, *2*(2), 475-481.