RSA VA ELGAMAL KRIPTOGRAFIK OCHIQ KALITLI ALGORITMLARNING QIYOSIY TAHLILI

Po’latov Doston Normurod o’g’li
Roziqov Abdug’ani Ilhomjon o’g’li
Jumaboyev Javlonbek Sherqul o’g’li
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Ushbu tezisda biz samaradorlikni sezilarli darajada oshiradigan Elliptik egri raqamli imzo algoritmiga asoslangan Raqamli imzo sxemasini taklif qilamiz. Bizning sxemamiz xavfsizligi Elliptik egri diskret logarifm muammosining qiyinligiga asoslangan. Shu sababli, u kerakli xavfsizlik darajalari uchun ancha kichikroq kalit uzunliklarini taklif qiladi, shu bilan birga kriptografik jarayonlar ancha tezlashadi, bu esa kamroq apparat va dasturiy ta'minot talablarini keltirib chiqaradi.*

Kalit so’zlar: *shifrlash algoritmlari, elektron raqamli imzo, RSA, ElGamal, DSA*

Abstract: *In this thesis, we propose a Digital Signature Scheme based on the Elliptic Curve Digital Signature Algorithm, which greatly improves efficiency. The security of our scheme is based on the difficulty of the elliptic curve discrete logarithm problem. Therefore, it offers much smaller key lengths for the required security levels, while the cryptographic processes are much faster, resulting in lower hardware and software requirements.*

Keywords: *encryption algorithms, electronic digital signature, RSA, ElGamal,DSA*.

KIRISH

Odamlar bugungi kunda Internet orqali uydan chiqmasdan turib, bank operatsiyalari kabi kundalik ishlarini bajarishlari mumkin. Odamlar xarid qilish ehtiyojlarini Internet orqali ham amalga oshiradilar, bu esa elektron tijoratning o'sish sur'atini oshirdi. So‟nggi vaqtlarda axborot texnologiyalari kundalik hayotimizga kirib, muhim hukumat loyihalaridan tortib oddiy maishiy muammolarni yechishni ham qamrab olmoqda. Yangi texnologiyalar cheksiz imkoniyatlar va kata foyda keltirishi bilan birgalikda yangi muammolarni ham paydo qilmoqda. Ulardan biri axborotni olishi mumkin bo‟lmagan shaxslar qo‟liga tushishidan himoyalash muammosidir. RSA algoritmining kuchi raqamlarni asosiy omilga ajratishda qiyinchilik darajasida. Ochiq kalit "n" - "p" va "q" o'zgaruvchilarida saqlangan ikkita raqamni ko'paytirish. "p" va "q" qiymatini aniqlash uchun faktorizatsiya jarayoni "n" qiymatiga bog'liq. Agar "n" faktorlar hisoblansa, "m" qiymatini aniqlash oson. "E" qiymati ma'lum bo'lsa-da, "d" kalitini hisoblash oson emas, chunki "m" qiymati noma'lum. RSA algoritmining afzalliklari turli xil hujumlardan, ayniqsa qo'pol kuch hujumlaridan himoya qilish tizimidir. Buning sababi shundaki, parolni hal qilishning murakkabligini kalit juftlik ishlab chiqarish jarayoni vaqtida katta "p" va "q" qiymatlarini aniqlash orqali aniqlash mumkin. Natijada "n" sezilarli bo'shliqni yaratadigan sezilarli raqam va buRSA ni hujumga chidamli qiladi. Biroq, shaxsiy kalitning o'lchami juda katta bo'lsa, shifrni ochish jarayoni

juda sekin bo'ladi, ayniqsa katta xabar o'lchamlari uchun. Shuning uchun, RSA odatda parol shifrlash va PIN raqami kabi kichik xabarlarni shifrlash uchun ishlatiladi.

ADABIYOTLARNI TUZISH

DES, 3DES, AES va RSA ni qiyosiy o'rganish

Internet va boshqa ommaviy axborot vositalari orqali ma'lumotlar almashinuvi odamlar uchun ma'lumot almashishda foydalidir. Ma'lumotni etkazib berish tez. Bu xavfsizlik hujumlaridan tizim himoyasini talab qiladi . Ma'lumotlarni o'z vaqtida yuborish uchun ko'plab usullardan foydalanish mumkin. Mualliflar kriptografiyani real vaqt rejimida xavfsizlik mexanizmlarini ta'minlash uchun qulay usul ekanligini ta'kidlaydilar.

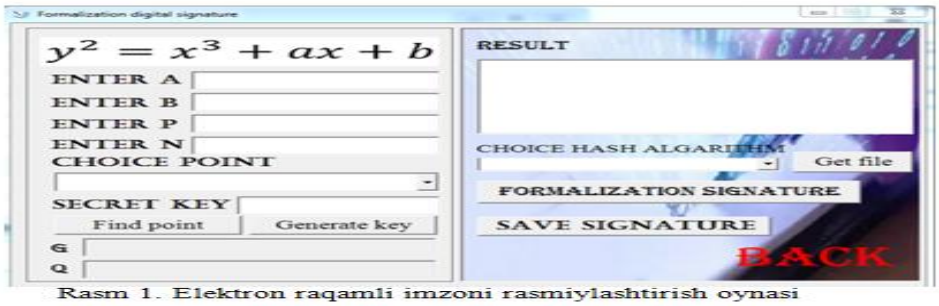
Kriptografiya yovvoyi partiyalardan ma'lumotlarni yashirish uchun ishlatiladi. Ularning tadqiqotlari DES, 3DES, AES va RSA algoritmlarini hujumlardan himoyalangan ma'lumotlarni himoya qilish qobiliyatiga qarab tahlil qiladi. Ma'lumotlarni himoya qilish tezligi va samaradorligi ham sinovdan o'tkaziladi.

Ushbu bo'limda simmetrik algoritmlar (DES, 3DES, AES) va RSA algoritmlari hamda ularning turli mazmun va o'lchamdagi kirish fayllarini shifrlashdagi ishlashi tahlil qilinadi. Tahlil natijalariga ta'sir etuvchi omillardan ba'zilari quyidagilardir.

•Hajmi. Har bir algoritm ishlashi uchun turli xil xotira sig'imlari talab qilinadi. Bu talab ochiq matnning o'lchami, aylanmalar soni va boshqalar bilan belgilanadi. Algoritm kichik xotiradan foydalangan holda, algoritm oddiy matnni muammosiz va tez qayta ishlay olsa yaxshi bo'ladi.

•Vaqt. Bu shifrlash va shifrni ochish jarayonini yakunlash uchun algoritm tomonidan talab qilinadigan vaqt miqdori. Protsessorning tezligi va algoritmning murakkabligi algoritmning ishlashiga ta'sir qiladi.

•Shifrlash va shifrni ochish bo'yicha o'tkazuvchanlik-o'tkazish algoritmi ochiq matnni umumiy vaqtga bo'lish yo'li bilan olinadi.



Rasm 1. Elektron raqamli imzoni rasmiylashtirish oynasi

Rasm 2. Raqamli imzoni tekshirish oynasi

Sinov natijasi shuni ko'rsatadiki, AES turli xil foydalanuvchi yuklarida soniyada so'rov jarayonlari soni va javob vaqtlari bo'yicha boshqa algoritmlarga qaraganda yaxshiroq. RSA va Triple DES ning yuqori quvvat sarfiga qaramay, AES yaxshi ishlash va xavfsizlikka ega. DES AESga qaraganda kamroq quvvat sarflaydi. Old DES eng zaif xavfsizlikka ega va atigi o'n besh soat ichida qo'pol kuch hujumlari bilan osongina echilishi mumkin. 128-bitli AES kaliti RSA 2600-bitli kalitlar bilan taqqoslanadigan kuchga ega. Bu AESni taqqoslangan algoritmlar orasida eng yaxshisi qiladi.

2.2 Ochiq kalitlarni shifrlash algoritmiga sharh

Kompyuter xavfsizligi yovvoyi tomonlardan axborot tizimlari resurslarining yaxlitligi, mavjudligi va maxfiyligini saqlashga xizmat qiladi [24][25]. Yuborilgan xabarning haqiqiyligi va to'g'riligi to'ldirilishi kerak, shunda qabul qiluvchi xabarni jo'natilgandek qabul qiladi. Xavotirli tomoni shundaki, xabarlarni jo'natish paytida xabarning o'zgarishi sodir bo'ladi. Ma'lumotlar maxfiyligi, ayniqsa, mamlakat ma'lumotlariga ega kompaniyalarda maxfiy saqlanishi kerak. RSA - bu autentifikatsiyani topshirish vaqtida ma'lumotlarning maxfiyligini saqlab qolishi mumkin bo'lgan algoritm. RSA dinamik kalitlarga ega, ular har safar kalitning generatsiyasiga qarab o'zgarishi mumkin [14][26].

Hung-Min Sun [27] tadqiqoti RSA ni dual tizim yordamida o'zgartirishga harakat qiladi. Ushbu tizim kalitlarni saqlashga bo'lgan ehtiyojni kamaytirishga xizmat qiladi. Muallifning ta'kidlashicha, RSA dual-tizimlarining kamchiliklari - kalitlarni yaratish algoritmlari ham optimallashtirilgan hisoblash murakkabligi.

Taher ElGamal diskret logarifmlarga asoslangan imzo sxemasini taklif qildi. U shifrlash va dekodlash jarayonlari uchun ochiq kalitni yaratish uchun Diffie-Hellman kalitlarni taqsimlash sxemasini amalga oshirdi. Kuchlilik cheklangan maydonlar bo'yicha diskret logarifmlarni hisoblash qiyinligiga bog'liq. Qanchalik ko'p son ishlatilsa, diskret logarifmlar shunchalik qiyin bo'ladi [15].

3. **NATIJA VA MUHOKAMA**

Tadqiqotchining ushbu bo'limi ikkita algoritmni solishtirishga va qaysi algoritm tezroq ekanligini aniqlashga va har bir algoritmning afzalliklarini izlashga harakat qiladi.

3.1 KALIT YARATISH

RSA oltita o'zgaruvchini ishlab chiqaradi (P, Q, N,Phi, E, D) kalit hosil qilish vaqtida. "N" va "E" o'zgaruvchilari shifrlash uchun, "N" va "D" esa shifrlash uchun ishlatiladigan kalitlardir. ElGamal kalit yaratish vaqtida to'rtta o'zgaruvchini (P, G, X, Y) ishlab chiqaradi. "P", "G" va "Y" o'zgaruvchilari shifrlash jarayonida, "P" va "X" o'zgaruvchilari shifrlash jarayonida ishlatiladi. Quyidagi misol RSA va ElGamal kalitlarini yaratishdir.

RSA

P = 5062283

Q = 6515623

N = P.Q

= 32983927547309

PH = (P-1).(Q-1)

= 32983915969404

E = 287

D = 11952359793791

ElGamal

P = 6062429

G = 1628134

X = 660876

$Y=G^X\%$ P

5809535

RSA va ElGamal kalit avlodida nisbatan bir xil vaqtga ega. Kalit yaratish unchalik katta bo'lmagan raqam uchun ko'p vaqt talab qilmaydi. RSA va ElGamal 2048 bitli kalitlarni yaratish uchun ko'proq vaqt talab etadi, chunki hisoblash natijasi modulli ifodaga ega bo'lishi kerak.

3.2 Shifrlash

Shifrlash bo'limida sinovdan o'tgan ochiq matn "UNIVERSITY"dir. Bu so'z ko'tarilgan kalitga ko'ra shifrlanadi. Bir nechta kalitlar turli uzunlikdagi kalitlar bilan yaratilgan.

IN	N	I	IN	VA	R	S	I	T	VA
85	78	73	86	69	82	83	73	84	89

RSA

P = 6713911561289923

Q = 8067467447266457

N = P.Q

```
      = 50298
 A[4] = (15442^39183) % 76481
        = 53509
B[4] = ((26297^39183) * 69) % 76481
      = 335
 A[5] = (15442^54480) % 76481
        = 56506
B[5] = ((26297^54480) * 82) % 76481
      = 62508
 A[6] = (15442^61237) % 76481
        = 43167
B[6] = ((26297^61237) * 83) % 76481
      = 34850
 A[7] = (15442^73115) % 76481
        = 56559
B[7] = ((26297^73115) * 73) % 76481
      = 71675
A[8] = (15442^48942) % 76481
      = 32727
B[8] = ((26297^48942) * 84) % 76481
      = 48351
A[9] = (15442^44474) % 76481
      = 41457
B[9] = ((26297^44474) * 89) % 76481
      = 65154

Shifrlangan matn:
50157 49769 68957 24976 17835 26125 23423 50298 53509 335 56506 62508 43167
34850 56559 71675 3415 3415

Vaqt: 1,2034075 soniya.
```

3.3 Shifrni ochish

Shifrni ochish jarayoni shifrlangan matnni ochiq matnga qaytaradi. Quyida RSA va ElGamal algoritmlarining shifrini ochish jarayoni keltirilgan.

```
RSA
P = 6713911561289923
Q = 8067467447266457
N = P.Q
      = 541642629645323678645232100128 11
PH = (P-1).(Q-1)
      = 541642629645323530831442014564 32
E = 733
D = 472921259171905947792800667559 57

  P1 =2009692949132817359093804310484 2^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 85
  P2 =4880176143763791548094795261801 6^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 78
  P3 =4822772508273232557900868393022 1^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 73
  P4 =1175401243690515152059385208538 4^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 86
  P5 =5180507213825957456948816585251 7^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 69
  P6 =8010444548914103342943171918866^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 82
  P7 =2905229440137993740772342597731 9^472921259171905947792800667559 57%
                541642629645323678645232100128 11
      = 83
  P8 =4822772508273232557900868393022 1^472921259171905947792800667559 57%
                541642629645323678645232100128 11
```

= 5416426296453236786452321001281 1
PH = (P-1).(Q-1)
= 5416426296453235308314420145643 2
E = 733
D = 472921259171905947792800667559 57

C1 = 85^{733}% 5416426296453236786452321001281 1
=200969294913281735909380431040 42
C2 = 78^{733}% 5416426296453236786452321001281 1
=488017614376379154809479526180 10
C3 = 73^{733}% 5416426296453236786452321001281 1
=482277250827323255790086839302 21
C4 = 86^{733}% 5416426296453236786452321001281 1
=117540124369051515205938520853 84
C5 = 69^{733}% 5416426296453236786452321001281 1
=518050721382595745694881658525 17
C6 = 82^{733}% 5416426296453236786452321001281 1
=801044454891410334294317191886 6
C7 = 83^{733}% 5416426296453236786452321001281 1
=290522944013799374072342597731 9
C8 = 73^{733}% 5416426296453236786452321001281 1
=482277250827323255790086839302 21
C9 = 84^{733}% 5416426296453236786452321001281 1
=390319227112291745449255190987 65
Q10 = 89^{733}% 5416426296453236786452321001281 1
=170240720628974695339249072574 0

Shifrlangan matn:
200969294913281735909380431040 42
488017614376379154809479526180 10
482277250827323255790086173232557900868391021515 3852085384
518050721382595745694881658525 17 801044454891410342943171918866
290522944013799374013792374027272727374272 7 32557900868393022 1
390319227112291745449255190987 65 170240720628974695339249072574 0
Vaqt: 0,0033971 soniya.

ElGamal
P = 76481
G = 15442
X = 30951
Y=G^X% P
15442^{30951}% 76481
26297

K[0] = 68490
K[1] = 42064
K[2] = 70103
K[3] = 25789
K[4] = 39183
K[5] = 54400
K[6] = 61237
K[7] = 73115
K[8] = 48942
K[9] = 44474

A[0] = (15442^{68490}) % 76481
= 50157
B[0] = ((26297^{68490}) * 85) % 76481
= 49769
A[1] = (15442^{42064}) % 76481
= 68957
B[1] = ((26297^{42064}) * 78) % 76481
= 24976
A[2] = (15442^{70103}) % 76481
= 17835
B[2] = ((26297^{70103}) * 73) % 76481
= 26125
A[3] = (15442^{25789}) % 76481
= 23423
B[3] = ((26297^{25789}) * 86) % 76481

4. **XULOSA**

RSA algoritmining shifrlash va shifrni ochish vaqti ElGamal algoritmiga qaraganda yaxshiroq. RSA shifrlangan matnda ElGamal algoritmiga qaraganda kamroq raqamlar mavjud. ElGamal algoritmida shifrlangan matn juftligi mavjud. Har bir shifrlangan ochiq matn ikkita shifrlangan matn qiymatini hosil qiladi. RSA algoritmi va ElGamal algoritmi assimetrik algoritmlar bo'lib, shifrlash va shifrni ochish uchun turli formulalarga ega. RSA algoritmi ElGamal algoritmiga qaraganda tezroq. Xavfsizlikka kelsak, ElGamal algoritmini RSA algoritmiga qaraganda echish qiyinroq bo'ladi, chunki ElGamal diskret logarifmlarni echish uchun murakkab hisob-kitoblarga ega.

FOYDALANILGAN ADABIYOTLAR:

1. Akkreditatsiya qilingan standartlar qo'mitasi X9, Amerika milliy standarti X9.62-2005,

Moliyaviy xizmatlar sanoati uchun ochiq kalit kriptografiyasi, Elliptik egri raqamli imzo algoritmi (ECDSA), 2005 yil 16 noyabr.

2. Certicom Research, Samarali kriptografiya standartlari, SEC 1: Elliptic Curve Cryptography, Versiya 2.0, 21 may, 2009 yil.

3. Lopez, J. va Dahab, R. Elliptik egri kriptografiyaga umumiy nuqtai, IC-00-10 texnik hisoboti, Kampinas davlat universiteti, 2000 yil.

4. N. Koblitz, —Eliptik egri kriptotizimlar‖, Hisoblash matematikasi, 48-son, 1987 yil.