RSA SHIFRLASH ALGORITMI VA BRUTE-FORCE HUJUM USULINING SAMADORLIGI

Nasriddinov Javohir Ismoiljon o‘g‘li
O‘zbekiston Milliy Universiteti I-bosqich magistranti
E-mail: *abdurrahmonumar6@gmail.com*

Annotatsiya: Bu ishda zamonaviy kriptografiyada keng qo‘llaniladigan RSA shifrlash algoritmini Brute-Force usuli yordamida buzish imkoniyatlari o‘rganiladi.Ish jarayonida RSA algoritmining matematik asoslari, kalitlar yaratish mexanizmlari hamda shifrlash va shifrdan ochish jarayonlarini to‘liq tahlil qilinadi. Brute-Force hujumi usuli bilan RSA kalitlarini topishning nazariy imkoniyatlari ko‘rib chiqiladi va bu usulning samaradorligi baholanadi.

Kalit so‘zlar:RSA, Brute-Force, kriptotahlil, tub sonlar,kriptografiya,Eyler funksiyasi

Аннотация: В данной работе изучаются возможности взлома широко используемого в современной криптографии алгоритма шифрования RSA методом Brute-Force. При этом полностью анализируются математические основы алгоритма RSA, механизмы генерации ключей, процессы шифрования и дешифрования. Рассматриваются теоретические возможности нахождения ключей RSA методом Brute-Force и оценивается эффективность данного метода.

Ключевые слова: RSA, Brute-Force, криптоанализ, простые числа, криптография, функция Эйлера

Abstract: This work studies the possibilities of cracking the RSA encryption algorithm, which is widely used in modern cryptography, using the Brute-Force method. In the process, the mathematical foundations of the RSA algorithm, key generation mechanisms, and the encryption and decryption processes are fully analyzed. The theoretical possibilities of finding RSA keys using the Brute-Force attack method are considered and the effectiveness of this method is evaluated.

Keywords: RSA, Brute-Force, cryptanalysis, prime numbers, cryptography, Euler function

Kirish

RSA shifrlash algoritmi ochiq va yopiq kalit asosida ishlaydigan shifrlash algoritmi hisoblanadi. Uning nomi algoritmni ishlab chiqqanlarning familiyalarining birinchi harfidan olingan, ya’ni Rivest, Shamir va Adleman. Bu shifrlash algoritmi berilgan yetarli katta bo‘lgan toq sonni ikki tub ko‘paytmasi sifatida ajratishning rastisonal usuli mavjud emasligiga asoslanib yaratilgan.

Brute-Force usuli bu berilgan muammoni yechimini aniqlash uchun mavjud bo‘lgan barcha variantlarni ketma-ket tekshirib chiqish usuli hisoblanadi.

ISSN 3030-3907

ADABIYOTLAR TAHLILI

Shifrlash ketma-ketligi quyidagicha:

1-qadam. Ikkita tub son p va q tanlab olinadi .

2-qadam. Ochiq kalit n hosil qilinadi:

$$n = p * q \ (1)$$

3-qadam. Eyler funksiyasi hisoblanadi:

$$f(p,q) = (p-1) * (q-1) \quad (2)$$

4-qadam. Eyler funksiyasining qiymati bilan o‘zaro tub bo‘lgan katta tub son d tanlab olinadi.

5-qadam. e soni aniqlanadi.

$$e * d \ mod \ f(p,q) = 1 \quad (3)$$

Yuqoridagi shartni bajaradigan e soni kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi.

6-qadam. Quyidagi formula orqali axborot shifrlanadi.

$$C_i = P_i^e mod \ n \quad (4)$$

Shifrni ochishda esa:

$$P_i = C_i^d mod \ n \quad (5)$$

formuladan foydalaniladi.

RSA algoritmida kalit uzunligini bitda hisoblash bevosita n ga bog‘liq:

$$L = [\log_2 n] + 1 \quad (6)$$

METODOLOGIYA

RSA algoritmini Brute-Force usulida yechish degani albatta, bizda faqatgina e soni va shifrlangan matn qiymatlari bor deb olinadi.Shuningdek, 10 ming ta inglizcha so‘zdan iborat maxsus lug’atimiz ham bor deb hisoblaylik.

Metodologiya bo‘yicha qilinadigan birinchi ish bu n sonining maksimal chegarasini tanlab olishdir. Keyingi qadamda 2 dan boshlab n gacha barcha sonlarni Sympy kutubxonasidagi factorint funksiyasi yordamida tub ko‘paytuvchilarga ajratib olinadi. Biz bu holatda Shor algoritmini tub ko‘paytuvchilarag ajratish uchun ishlatishimiz mumkin edi. Lekin Shor algoritmi kvant kompyuterlar uchun ishlatiladi, klassik kompyuterlarda bu algoritmdan foydalanish qiyinchilik tug‘diradi.

Shart sifatida aniqlangan tub ko‘paytuvchilarning soni 2 taga tengligi olinadi.Undan keyingi shartda shu ikki sonning ko‘paytmasi n ga tengligi tekshiriladi.

Bu shartlar ham bajarilsa, Eyler funksiyasi hisoblanadi.Eyler funksiyasi aniqlangandan keyin unga bog‘liq d soni aniqlanadi. d soni topildi deb olsak, shu topilgan qiymat bilan shifrni ochamiz. Ochilgan shifrmatnni qaytadan shifrlaymiz. Shifrlangan matn bizga berilgan shifrmatnga ustma-ust tushsa va deshifrlangan

ISSN 3030-3907

matn bizning lug‘atimizda mavjud bo‘lsa, biz topgan n shifrlashda ishlatilgan n ga teng.

Kriptotahlilning bu usulida shifrmatn va shifrlash algoritmi va bitta kalit bor deb hisoblanib, kalit haqida ma’lumotga ega bo‘lish maqsadida shifrmatnni tahlil qilish va ochiq matnni topishga urinishdan iboratdir.

Misol tariqasida, e=11 bo‘lgan holatni qaraymiz. n=100697 (p=101, q=997) holatda P=“unsuccessful” so‘zini shifrlaymiz:

Ochiq matndagi har bir harfni ASCII jadvalidagi kodini olamiz:

1-jadval

Matn elementlarining ASCII jadvalidagi berilishi

u	117	e	101
n	110	s	115
s	115	s	115
u	117	f	102
c	99	u	117
c	99	l	108

Endi har bir qiymat uchun C_i lar hisoblanadi.

$$C_0 = 117^{11} mod\ 100697 = 31078$$
$$C_1 = 110^{11} mod\ 100697 = 38934$$
$$C_2 = 115^{11} mod\ 100697 = 96873$$
$$C_3 = 117^{11} mod\ 100697 = 31078$$
$$C_4 = 99^{11} mod\ 100697 = 60168$$
$$C_5 = 99^{11} mod\ 100697 = 60168$$
$$C_6 = 101^{11} mod\ 100697 = 35350$$
$$C_7 = 115^{11} mod\ 100697 = 96873$$
$$C_8 = 115^{11} mod\ 100697 = 96873$$
$$C_9 = 102^{11} mod\ 100697 = 2728$$
$$C_{10} = 117^{11} mod\ 100697 = 31078$$
$$C_{11} = 108^{11} mod\ 100697 = 34694$$

Natijani umumiy ko‘rinishda yozsak:

$$C = [31078, 38934, 96873, 31078, 60168, 60168, 35350, 96873, 96873, 2728, 31078, 34694].$$

Bu berilgan ochiq kalitlardan foydalangan holda hosil bo‘lgan shifrmatndir. Buni ochish uchun esa d yopiq kalit topiladi.

Bizning misolimizda, e=11 va n=100697. d shunday sonki, u hamda e ning ko‘paytmasini Eyler funksiyasiga bo‘lganda qoldiq 1 ga teng bo‘lishi shart. Bizda Eyler funksiyasi noma’lum. p va q lar orqali hisoblanishi hisobiga, n sonini ikki tub son ko‘paytmasi ko‘rinishida tasvirlash zarurati tug‘iladi.

ISSN 3030-3907

Buning oson va tushunarli usuli bu 100697 ni tub sonlarga bo‘lib chiqishdir. Avvalo, 100697 dan ildiz olinadi. Bu taxminan 317 atrofidagi son bo‘ladi. Endi 100697 ni 317 gacha bo‘lgan tub sonlarga bo‘lib chiqamiz. Natija o‘rnida p=101 va q=997 qabul qilinadi.

Eyler funksiyasi $f(101,997) = (101-1) * (997-1) = 99600.$

$$11 * d \; mod \; 99600 = 1.$$

Yuqoridagi tenglamadan d ni topish mumkin va uni ikki variantda ko‘rish mumkin:

1-variant. 99600 ni 1 dan boshlab natural sonlarga ko‘paytirish va natijaga birni qo‘shib, yig‘indini 11 ga qoldiqsiz bo‘ladigan sonni aniqlash;

2-variant. 11 ni 1 dan boshlab sonlarga ko‘paytirish va 99600 ga bo‘lganda 1 qoldiqqa erishadiganida to‘xtash.

1-variantda ko‘rishimiz mumkin:

2-jadval

d sonini topish

Iteratsiya	Yig‘indi	[d]	Qoldiq
1	99601	9054	7
2	199201	18109	2
3	298801	27163	8
4	398401	36218	3
5	498001	45272	9
6	597601	54327	4
7	697201	63381	10
8	796801	72436	5
9	896401	81491	0

2-jadvaldan ma’lumki, 99600*9+1=11*81491 ekan. Ya’ni qoldiqsiz bo‘linadigan birinchi son d=81491.

Deshifrlash jarayoni.

$$P_0 = 31078^{81491} mod \; 100697 = 117 \rightarrow 'u'$$
$$P_1 = 38934^{81491} mod \; 100697 = 110 \rightarrow 'n'$$
$$P_2 = 96873^{81491} mod \; 100697 = 115 \rightarrow 's'$$
$$P_3 = 31078^{81491} mod \; 100697 = 117 \rightarrow 'u'$$
$$P_4 = 60168^{81491} mod \; 100697 = 99 \rightarrow 'c'$$
$$P_5 = 60168^{81491} mod \; 100697 = 99 \rightarrow 'c'$$
$$P_6 = 35350^{81491} mod \; 100697 = 99 \rightarrow 'e'$$
$$P_7 = 96873^{81491} mod \; 100697 = 115 \rightarrow 's'$$
$$P_8 = 96873^{81491} mod \; 100697 = 115 \rightarrow 's'$$

ISSN 3030-3907

$$P_9 = 2728^{81491} mod\ 100697 = 102 \rightarrow 'f'$$
$$P_{10} = 31078^{81491} mod\ 100697 = 117 \rightarrow 'u'$$
$$P_{11} = 34694^{81491} mod\ 100697 = 108 \rightarrow 'l'$$

Natijalarni birlashtirsak, “unsuccessful” so‘zi hosil bo‘ladi.

NATIJALAR

```
2025-06-09 13:30:47.408264
[81, 2, 98, 123, 118, 22, 73]
n topildi: 187
[81, 2, 98, 123, 118, 22, 73]
[81, 2, 98, 123, 118, 22, 73]
p: 11, q: 17, phi(n): 160, d: 37
Asl xabar: subject
2025-06-09 13:30:47.414398
```

1-rasm. . n=187 holatda dastur natijasi

Python dasturlash tilida yozilgan dastur yaratilgan. Shu dasturga “subject” so‘zini e=13 va n=187 holatda shifrlangan holati berilgan. Bunda kalit uzunligi $L = [\log_2 187] + 1 = 8$ bit. Bunda n_max=200 deb olingan. Natijadan ko‘rinib turibdiki, 0.006 ms vaqt ichida shifrmatn yechildi.

```
2025-06-09 13:19:39.436361
[606, 832, 115, 1740]
n topildi: 1919
[606, 832, 115, 1740]
[606, 832, 115, 1740]
p: 19, q: 101, phi(n): 1800, d: 491
Asl xabar: easy
2025-06-09 13:19:39.478422
```

2-rasm. n=1919 holatda dastur natijasi

Birinchi tajribada, P=“easy” so‘zini n=1919(kalit uzunligi L=11 bit) holatda e=11 da shifrlab ko‘rdik. C=[606,832,115,1740] hosil bo‘lgan shifrmatnni n_max=2000 holatda yechishga urindik. p=19 va q=101 ekanligini aniqlashga 0.04 ms vaqt ketdi.

```
2025-06-09 13:39:00.322196
[31078, 38934, 96873, 31078, 60168, 60168, 35350, 96873, 96873, 2728, 31078, 34694]
n topildi: 100697
[31078, 38934, 96873, 31078, 60168, 60168, 35350, 96873, 96873, 2728, 31078, 34694]
[31078, 38934, 96873, 31078, 60168, 60168, 35350, 96873, 96873, 2728, 31078, 34694]
p: 101, q: 997, phi(n): 99600, d: 81491
Asl xabar: unsuccessful
2025-06-09 14:40:02.481985
```

3-rasm. n=100697 holatda dastur natijasi

Ko‘rinib turganidek, dastur ishlashni boshlagan vaqtdan to tugaguncha 61 daqiqa vaqt ketgan. Albatta, bu tajribada kalit uzunligi 17 bit. Natijalar quyidagicha:

$$n = 100697, p = 101, q = 997$$
$$f(p, q) = 99600$$
$$d = 81491$$

Deshifrlangan matn esa “unsuccessful” bo‘ldi.

ISSN 3030-3907

3-jadval

Natijalar

n	Kalit uzunligi	Vaqt
187	8 bit	0.006 ms
1919	11 bit	0.04 ms
100697	17 bit	61 daqiqa

XULOSA

RSA shifrlash algoritmini buzish uchun Brute Force hujum usuli kalit uzunligi juda ham kichik bo‘lgan holatda ishlaydi. Biz o‘tkazgan tajribalarda kalit uzunligi maksimal holatda 17 bit uzunlikda olingan, shunda ham dastur shifrni yechgunicha 1 soatdan ko‘proq vaqt ajratdi.

Odatda, 2048 yoki 4096 bitli kalit ishlatilishini hisobga olsak, bu yerda juda ham ko‘p kombinatsiyalar ishlatiladi. Bu holatda oddiy kompyuterda Brute-Force usuli bilan milliard yilda ham ochish imkonsiz. Shu hisobdan bu hujum usuli RSA algoritmiga nisbatan samarasiz.

Hozirgi zamonda tub sonlarga ajratishning boshqacha algoritmlari, masalan kvant kompyuterlar uchun Shor algoritmi ishlatilishini hisobga olinsa, axborot xavfsizligining asosiy tayanchlaridan biri bo‘lgan RSA shifrlash algoritmi ham jiddiy xavf ostida qoladi. Buni hisobidan, yangi kvant hujumlarga bardoshli kriptografik algoritmlar ustida tadqiqotlar davom ettirilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. Zabihullah Zahir, “RSA Public Key Cryptosystem”, JARIIE-ISSN(O)-2395-4396 Vol-6 Issue-4 2020 1680-1685 pages
2. D. Y. Akbarov, P. F. Xasanov, X. P. Xasanov, O. P. Axmedova, I. U. Xolimtayeva , “KRIPTOGRAFIYANING MATEMATIK ASOSLARI”, Toshkent 2018 yil, 192 bet
3. S.K.Ganiyev, M.M.Karimov, K.A.Tashev, “Axborot xavfsizligi”, Toshkent - 2016 yil, 366 bet
4. Ikhwan Al Hakim , “Analyzing the Time Complexity of RSA Encryption Cracking Using the Brute Force Method”, Makalah IF2120 Matematika Diskrit – Sem. I Tahun 2023/2024
5. I.M. Boyquziyev, “ZAMONAVIY KRIPTOTAHLIL USULLARI”, Toshkent-2025 yil, 239 bet
6. Noel Christoffel Simbolon, “Rudimentary Cryptanalysis of the Affine Cipher with Known Alphabet Size using the Brute-Force Algorithm”, IF2211 Algorithm Strategies Paper, 2nd Semester, 2022/2023

ISSN 3030-3907