Ergashev Isroilbek Abdirashid o‘g‘li
Chirchiq davlat pedagogika universiteti
“Matematika o‘qitish metodikasi va geometriya” kafedrasi o‘qituvchisi.
E-mail: isroilbek19960818@gmail.com

RSA ASIMMETRIK SHIFRLASH ALGORITMINING MURAKKABLIGI.

Annotatsiya: Mazkur maqolada asimmetrik shifrlash algoritmlar turkumiga kiruvchi RSA shifrlash algoritmining asosiy murakkabliklari va ularga muqobil murakkabliklarni aniqlash masalasi bo‘yicha tadqiqotlar va ularning natijalari keltirilgan.

Kalit so‘zlar: RSA, Eyler funksiyasi, matematik murakkablik, tub sonlar, faktorizatsiya.

Эргашев Исроилбек Абдирашид угли
Чирчикский государственный педагогический университет
Преподаватель кафедры “Методики преподавания математики и геометрии”.

СЛОЖНОСТЬ АЛГОРИТМА АСИММЕТРИЧНОГО ШИФРОВАНИЯ РСА.

Аннотация: В данной статье представлены исследования и их результаты по вопросу определения основных сложностей алгоритма шифрования RSA, относящегося к группе алгоритмов асимметричного шифрования, и альтернативных сложностей.

Ключевые слова: РСА, функция Эйлера, математическая сложность, простые числа, факторизация.

Ergashev Isroilbek Abdirashid o‘g‘li
Chirchik State Pedagogical University
teacher of the “Methodology of mathematics teaching and geometry” department.

COMPLEXITY OF RSA ASYMMETRIC ENCRYPTION ALGORITHM.

Abstract: This article presents research and their results on the issue of determining the main complexities of the RSA encryption algorithm, which belongs to the group of asymmetric encryption algorithms, and alternative complexities.

Keywords: RSA, Eyler's function, mathematical complexity, prime numbers, factorization.

Kirish

1977 yilda R. L. Rayvest, A. Shamir va L. Adleman «Method for Obtaining Digital Signatures and Public Key Cryptosystems» deb ataluvchi ilmiy maqolalarida Diffi va Xellman g‘oyalarining amaliy tadbiqi sifatida RSA nomi bilan ataluvchi asimmetrik kriptosistemaga asoslangan umumiy shifrlash algoritmini taklif etgan edilar. RSA kriptotizimining bardoshlilik darajasi berilgan sonni ikkita tub ko‘paytuvchilar ko‘paytmasiga yoyishning qiyinchilik darajasiga ekvivalentdir.

Adabiyotlar tahlili

Faktorlash muammosining yuzaga kelishi antik davrlarga, Eratosfen yashagan davrlarga, taxminan, eramizgacha 284-202 yillarga to‘g‘ri keladi, muammoning undan keyingi tarixi Fibbanochi (taxminan 1180-1250 yy.), Ferma (1601-1665 yy.), Eyler (1707-1783 yy), Lejandr (1752-1833 yy.), Gauss (1777-1855 yy.) kabi ulug‘ matematiklar nomi bilan bog‘langan [4].

Faktorlash muammosini hal etishda $n$modulni faktorlash masalasini yechishda birinchi navbatda hayolga keladigan usul, bu $\sqrt{n}$ dan oshmaydigan tub sonlarni tanlab ularga bo‘lib ko‘rishdir. Boshqa tanlash usuli Fermaga tegishli bo‘lib, n ni kvadratlar ayirmasi ko‘rinishida ifodalashga asoslangan [1,2]:

$$n=a^2-b^2=(a+b)(a-b).$$

Ferma eng katta umumiy bo‘luvchi - $EKUB(n,a-b)$ ni, ya’ni $n$ning natural bo‘luvchisini topishga harakat qilishni hamda bunga imkon beruvchi usulni ham taklif etgan. Agar n ning ko‘paytuvchilari bir-biridan katta farq qilmasa, bu usul oddiy tanlash usuliga nisbatan tez yechim beradi va uning murakkabligi $O(\sqrt{n})$ ko‘rinishida

ifodalanadi, ammo hozirgi kunda kriptografik tizimlarda amalda foydalaniladigan hollar uchun ahamiyatga ega emas. Lejandr mazkur yondashuvda $a^2 \equiv b^2 (mod\, n)$ ga ega bo‘lish lozimligiga e’tibor qaratgan. Ammo, keltirilgan taqqoslama har qanday n uchun yetarli emasligini ham ko‘rsatgan va ko‘zlangan maqsadga erishish uchun uzluksiz kasrlardan foydalanish yo‘lini taklif etgan.

Kompyuterlar asrida dastlabki 1970 yillarda taklif etilgan faktorlash algoritmlaridan biri (p-1) Pollard algoritmi bo‘lgan. Undan so‘ng (p+1) Vilyams algoritmi va EEChlardan foydalanishga asoslangan Lenstra algoritmi ishlab chiqildi. Keyinchalik (p-1) Pollard algoritmi (p+1) Pollard algoritmi sifatida, Pollard r -, (- usuli nomlari ostida takomillashtirildi. r - (Pollard usulining murakkabligi $I_p = q/4$) amal bilan belgilanadi. Hozirgi kunga kelib, faktorlash muammosining eng tezkor usullari bo‘lib, chiziqli g‘alvir, kvadratik g‘alvir, sonli maydon g‘alviri, umumlashgan sonli maydon g‘alviri usullari tan olingan.

Hozirgi kunda eng samarali kriptotahlil algoritmlarining murakkabligi eksponensial emas, balki subeksponensial murakkablikka ega [1].

Algoritm eksponensial murakkablikka ega deyiladi, agarda uning murakkabligi qiymatining tartibi $O(t^{f(n)})$ bo‘lsa.

Algoritm polinomial murakkablikka ega deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n^m)$ bo‘lsa. Subeksponensial murakkablikka ega bo‘lgan algoritm murakkabligi qiymatining tartibi $O(n^m)$va $O(t^{f(n)})$ orasida bo‘ladi.

RSA shifrlash algoritmi va uning murakkabligi bo‘yicha ko‘plab tadqiqot ishlari olib borilgan [1-10].

Tadqiqot metodologiyasi

RSA shifrlash algoritmida ikkita p va q tub sonlardan foydalaniladi. $n = p * q$, $\varphi(n) = (p-1) * (q-1)$ Eyler funksiyasi hisoblanadi. $EKUB(d, \varphi(n)) = 1$ (1) shartni qanoatlantiruvchi e soni va $e * d = 1 \, mod \, \varphi(n)$ (2) shartni qanoatlantiruvchi d soni hisoblanadi.$(2, \varphi(n))$ oraliqda (1) shartni qanoatlantiruvchi bir qancha e sonlar va

aniqlangan e sonlar bilan birgalikda (2) shartni qanoatlantiruvchi shuncha d sonlar mavjud.

$C = M^e \bmod n$ ifoda bilan M ochiq ma'lumotni shifrlash jarayoni amalga oshirilsa, $M = C^e \bmod n$ ifoda bilan esa shifrmatndan ochiq ma'lumotni hosil qilish jarayoni amalga oshiriladi.

Misol: $p = 59$, $q = 71$, $n = 4189$, $\varphi(n) = 4060$

(1) va (2) tengliklarni qanoatlantiruvchi $e = 2137$, $d = 2713$ sonlari tanlab olinishi mumkin. $M = 237$ ma'lumotni shifrlash va shifrmatnni ochish jarayonlari quyidagicha amalga oshiriladi:

$237^{2137} \bmod 4189 = 1712$ shifrmatn hosil qilinadi.

$1712^{2713} \bmod 4189 = 237$ bu esa ochiq matnni hisoblash jarayoni.

Bir qarashda hammasi joyida, lekin, quyidagi $1712^{683} \bmod 4189 = 237$ ifodaning o'rinli ekanligi bu jarayonda ochiq matnni faqat $d = 2713$ soni bilan emas, balki $d' = 683$ kalit bilan ham aniqlash mumkinligini ko'rsatadi.

Agar yuqorida tanlab olingan tub sonlar uchun (1) va (2) tengliklarni qanoatlantiruvchi $e = 151$, $d = 2151$ sonlari tanlab olinsa yuqoridagi M ma'lumotni shifrlash va shifrni ochish jarayoni quyidagicha bo'ladi:

$237^{151} \bmod 4189 = 178.$

$178^{2151} \bmod 4189 = 237.$

Hisoblangan shaxsiy kalitdan tashqari $d' = 121$ kalit bilan ham dastlabki ochiq matnni hisoblash mumkin:

$178^{121} \bmod 4189 = 237.$

Natijalar

Umuman olganda tajribalar bunday e', d' sonlar jufti $p = 59$ va $q = 71$ tub sonlar jufti uchun emas balki boshqa p va q sonlar tanlab olinganda ham bir qancha ekanligini ko'rsatdi. Bir qancha p va q tub sonlar va M ma'lumot uchun tajribalarda aniqlangan yuqoridagi kabi biri bilan shifrlangan ma'lumotni boshqasi bilan ochish

mumkin bo‘lgan e, d va e', d' juftliklarning ayrim qiymatlari quyidagi jadvalda keltirilgan.

p, q, **M**	e, d,	e', d'	e, d	e', d'	e, d	e', d'
59,71, 1000	183,2507	2213,477	2217,1053	187,3083	2223,3187	193,1157
59,71, 17	123,4027	703,2287 993,3737 1283,2867 1573,1417 1863,547 2153,1997 2733,257 3023,1707 3313,837 3603,3447 3893,2577	129,2329	419,3779 709,2909 999,1459 1289,589 1579,2039 2159,299 2449,1749 2739,879 3029,3489 3319,2619 3609,9	2459,459	139,3359 429,2489 719,1039 1009,169 1299,1619 1879,3939 2169,1329 2749,3069 3039,2199 3329,3649 3909,1909
37,41, 65	1433,617	1073,977 1433,617	1439,1439	719,719 1079,359	1339,499	619,1219 979,859
37,41, 17	319,799	679,439	389,1229	29,149 1109,509	793,937	73,217 433,1297
127,151,237	3223,2287	73,5437	6473,13037	173,437	6653,1517	353,7817
127,151, 17	11,8591	3161,5441 6311,2291 9461,18041 12611,14891 15761,11741	47,15683	3197,12533 6347,9383 9497,6233 12647,3083 15797,18833	139,4759	3289,1609 6439,17359 9589,14209 12739,11059 15889,7909

1-jadval

Yuqoridagi 1-jadvaldan ko‘rish mumkinki ayrim hollarda bitta e, d kalitlar bilan shifrlangan M ma’lumotni aniqlash uchun bir qancha e', d' jufti mos kelishi kuzatildi, hattoki $p=127, q=151$ va $M=2$ holatda bitta e, d juftiga 45 ta e', d' jufti, $e=53, d=17117$ kalitlar tanlanganda esa 89 ta boshqa kalitlardan foydalanib dastlab ochiq matnni hosil qilish mumkinligi aniqlandi.

№	**73, 5437**	**169,18229**	**53,17117**	
1.	283,7747	379,11719	263,6827	9713,16277

2.	703,12367	799,17599	473,2837	9923,12287
3.	1123,10687	1219,17179	683,5147	10133,14597
4.	1543,2707	1639,10459	893,13757	10343,4307
5.	1963,7327	2059,16339	1103,9767	10553,317
6.	2383,5647	2479,15919	1313,12077	10763,2627
7.	2803,16567	2899,9199	1523,1787	10973,11237
8.	3223,2287	3319,15079	1733,16697	11183,7247
9.	3643,607	3739,14659	1943,107	11393,9557
10.	4063,11527	4159,7939	2153,8717	11603,18167
11.	4483,16147	4579,13819	2363,4727	11813,14177
12.	4903,14467	4999,13399	2573,7037	12023,16487
13.	5323,6487	5419,6679	2783,15647	12233,6197
14.	5743,11107	5839,12559	2993,11657	12443,2207
15.	6163,9427	6259,12139	3203,13967	12653,4517
16.	6583,1447	6679,5419	3413,3677	12863,13127
17.	7003,6067	7099,11299	3623,18587	13073,9137
18.	7423,4387	7519,10879	3833,1997	13283,11447
19.	7843,15307	7939,4159	4043,10607	13493,1157
20.	8263,1027	8359,10039	4253,6617	13703,16067
21.	8683,18247	8779,9619	4463,8927	13913,18377
22.	9103,10267	9199,2899	4673,17537	14123,8087
23.	9523,14887	9619,8779	4883,13547	14333,4097
24.	9943,13207	10039,8359	5093,15857	14543,6407
25.	10363,5227	10459,1639	5303,5567	14753,15017
26.	10783,9847	10879,7519	5513,1577	14963,11027
27.	11203,8167	11299,7099	5723,3887	15173,13337
28.	11623,187	11719,379	5933,12497	15383,3047
29.	12043,4807	12139,6259	6143,8507	15593,17957
30.	12463,3127	12559,5839	6353,10817	15803,1367
31.	12883,14047	12979,18019	6563,527	16013,9977
32.	13303,18667	13399,4999	6773,15437	16223,5987
33.	13723,16987	13819,4579	6983,17747	16433,8297
34.	14143,9007	14239,16759	7193,7457	16643,16907
35.	14563,13627	14659,3739	7403,3467	16853,12917
36.	14983,11947	15079,3319	7613,5777	17063,15227
37.	15403,3967	15499,15499	7823,14387	17273,4937
38.	15823,8587	15919,2479	8033,10397	17483,947
39.	16243,6907	16339,2059	8243,12707	17693,3257
40.	16663,17827	16759,14239	8453,2417	17903,11867
41.	17083,3547	17179,1219	8663,17327	18113,7877

42.	17503,1867	17599,799	8873,737	18323,10187
43.	17923,12787	18019,12979	9083,9347	18533,18797
44.	18343,17407	18439,18859	9293,5357	18743,14807
45.	18763,15727	18859,18439	9503,7667	

2-jadval

Yuqoridagi keltirilgan 2-jadvalda ochiq va yopiq kalitlar istalgan tartibda tanlanganda ham biri bilan shifrlangan $M=2$ ma'lumotni boshqasi bilan ochish mumkin.

$p=127, q=151$ tub sonlar uchun $e=3349, d=649$ kalitlar bilan shifrlangan har qanday M ma'lumotni $e'=199, d'=3799$ kalitlar bilan ochish mumkinligini ko'rsatdi.

$p=37, q=41$ tub sonlar uchun $e=887, d=263$ $e=883, d=663$ yoki ochiq va yopiq kalitlar juftlari tanlanganda $M=8$ ma'lumotni shifrlash va shifrni ochish uchun 16 tadan e', d' kalitlar juftlari mavjudligi ham aniqlandi.

Bu sonlarning takrorlanishi qanday qoida asosida paydo bo'layotganligi bo'yicha izlanishlar olib borildi.

Natijalar tahlili

T esa $a^t \bmod n \equiv 1$ shartni qanoatlantiradigan t sonlar to'plami belgilab olindi. $a=2$ uchun $a^t \bmod n \equiv 1$ tengliklar hisoblanganda aniqlanadigan T sonlar to'plamida $\varphi(n)$ sonining bo'luvchilari yotadi.

p	q	n	$\varphi(n)$	T
127	151	19177	18900	{105,210,315,420,525,630,735,840,945,1050,1155,1260,1365,1470,1575,1680,1785,1890,1995,2100,2205,2310,2415,2520,2625,2730,2835,2940,3045,3150,…}
59	71	4189	4060	{2030,4060,…}
37	41	1440	1517	{180,360,540,720,900,1080,1260,1440,…}
7	19	133	108	{18,36,54,72,90,108,126,…}
3	11	33	20	{10,20,…}
11	13	143	120	{60,120,…}
17	31	527	480	{40,80,120,160,200,240,280,320,360,400,440,480,…}
7	11	77	60	{30,60,…}

5	11	55	40	{20,40,…}
137	131	17947	17680	{4420,8840,13260,…}
61	53	3233	3120	{780,1560,2340,3120}

3-jadval

Yuqorida keltirilgan 3-jadvaldagi t ning bitta qiymati aniqlansa qolgan qiymatlari aniqlangan songa karrali qiymatlar bo‘ladi.

Bu aniqlangan to‘plam qiymatlaridan qanday foydalanish mumkin:

1. $\varphi(n)$ funksiyaning qiymatlarini T to‘plam elementlariga bo‘linadigan sonlar ichidan izlash zarur;

2. To‘plamning har bir t elementlari uchun dastlab aniqlangan e soni uchun e' sonni aniqlash $e'=e\pm t$ ifoda orqali aniqlanadi.

Kalitlarning mos kelishi xususiy holatlar uchun har t siklda qaytariladi. $t=EKUK(p-1,q-1)$ $a^t \bmod n\equiv 1$ tenglikdagi barcha a lar uchun o‘rinli bo‘ladi.

Barcha a lar uchun o‘rinli bo‘ladigan e' va d' ning barcha qiymatlari quyidagi tengliklar orqali aniqlanadi:

$$e'=e\pm k*m, k=1,2,3,\dots$$

$$d'=d\pm j*m, j=0,1,2,\dots \qquad (1)$$

bu yerda $m=EKUK(p-1,q-1)$.

Umuman olganda algoritmning murakkabligi $2^t \bmod n\equiv 1$ yoki $2^t \bmod (n-1)\equiv 0$ ifodalardan t sonini aniqlash masalasiga keladi.

$C=M^e \bmod n$ ifoda bilan shifrlangan M ma’lumotni $M=C^d \bmod n$ ifoda bilan hisoblash mumkin. (1) ifodaga ko‘ra $M=C^{d+j*m} \bmod n$ ($j=0,1,2,\dots$) tenglik ham o‘rinli.

Bundan esa $M=C^d*C^{j*m} \bmod n=(M*C^{j*m}) \bmod n$ ($j=0,1,2,\dots$) tenglik kelib chiqadi. Demak, $C^{j*m} \bmod n=1$ ($j=0,1,2,\dots$) tenglik o‘rinli.

Xulosa

Bu tajribalar natijalaridan xulosa qilish mumkinki, RSA shifrlash algoritmida shifrlangan ochiq kalitlar va ularga mos maxfiy kalitlarning takrorlanishi EKUK(p-1,q-1) qadamda takrorlanishi kuzatiladi. Bundan esa ikki xil ochiq kalit bilan shifrlangan ma’lumotlarning mos kelishi kamida ikkita kalit uchun kuzatiladi. Shu nuqtai nazardan mazkur algoritmning murakkabligi bo‘yicha tadqiqotlarni muntazam davom ettirish maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. Talbot, John and Dominic Welsh. Complexity and Cryptography. Cambridge: Cambridge University Press, 2006.
2. Rothe, Jörg. Complexity Theory and Cryptology. Berlin: Springer, 2005.
3. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
5. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.
6. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004.
7. ElGamal T. On computing logarithm over finite fields // Advances in cryptology —CRYPTO‘85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). – Pp. 396-402.
8. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Pp. 469-472.
9. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.:Лори Вильямс, 2001.
10. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.