Attacking The RSA Algorithm on Gaussian Integers by Using Continued Fractions

Wael Mahmood Abbas **1**$^{\text{st}}$ Ghufran A. Ghadhban 2$^{\text{nd}}$ and Hind A. majeed 3$^{\text{nd}}$

1 Department of Mathematics, college of science, University of Diyala, Diyala, Iraq.

2 Department of Mathematics, college of science, University of Diyala, Diyala, Iraq.

3 Mustansiriyah University College of Science, Physics department

[1]E-mail: w_alhayat@yahoo.com
[2]E-mail: ghofran_ali@uodiyala.edu.iq

[3]E-mail: hind88.hh@gmail.com

Attacking The RSA Algorithm on Gaussian Integers by Using Continued Fractions

Wael Mahmood Abbas 1st Ghufran A. Ghadhban 2nd and Hind A. majeed 3nd

1 Department of Mathematics, college of science, University of Diyala, Diyala, Iraq.

2 Department of Mathematics, college of science, University of Diyala, Diyala, Iraq.

3 Mustansiriyah University College of Science, Physics department

[1]E-mail: w_alhayat@yahoo.com
[2]E-mail: ghofran_ali@uodiyala.edu.iq

[3]E-mail: hind88.hh@gmail.com

Abstract

In this paper, we will study the method of attacking RSA on gaussian integer Since d is the inverse of e mod ø(N), we can figure out d if we know and the public key (the modulus n and the encryption exponent e) We can use the Extended Euclidean algorithm Knowing now is comparable to knowing P and Q, the two prime factors of N, mathematically speaking using continued fraction, The Wiener attack against the RSA cryptosystem with a small secret exponent is an application of this finding. Then, we show that regardless of the choice of N, there exists an attack based on continued fractions that recovers the secret exponent.

Introduction

A new method of attacking RSA, known as the modified Wiener's attack, has been proposed. This method operates in the domain of integers and converts the problem to the domain of Gaussian integers. By finding the appropriate starting asymptote, a new continuous fraction is used for estimating the trace from encoding and decoding messages.

If the secret exponent (d) contains at most one-fourth as many bits as the modulus (N), it is possible to crack a typical RSA cryptosystem efficiently. In this scenario, P and Q are Gaussian integers of the same size, and the public exponent (e) is less than N.

The basic relationship between exponents is used as the starting point for the Wiener's attack. If N(P) < N(Q) < 2N(P), e < N, and d is the denominator of a convergent from the continued fraction expansion of e/N, then there exists an integer k such that e*d - k*φ(N) = 1.

Approximately, φ(N) is equal to N, which implies that (k/d) is approximately equal to e/N. More precisely, we have the inequality $\mathcal{N} - 3\sqrt{N} < \varphi(N) < \mathcal{N}$.1. Continued fraction:

The faction $\frac{A}{B}$ can be expressed as a simple continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a2 + \cfrac{1}{a3 + \cfrac{1}{a4 + \ldots\ldots \cfrac{1}{an - 1 + \cfrac{1}{an}}}}}}$$

Were, a_0, a_1, a_2, . . ., a_n be real numbers. is called a finite continued fraction and is denoted by [a_0,a_1 , a_2,. . . , a_n]. A simple continued fraction can either finite or infinite the following example shows how to use Euclidian Algorithm.

Example 1:z Let us find the continued fraction expansion for $\frac{67}{29}$ = **[2,3 , 4,2**]

$$= 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}} = \frac{67}{29}$$

2.convegent:

In some sense, the convergent are the best possible approximations for a given nonnegative real:

Definition 1. We call [q_0, ..., q_m] (for $0 \leq m \leq n$) the m^{th} convergent to [q_0, ..., q_n]. In our example, the convergent are

$$A_0 = \frac{P_0}{Q_0}$$

$$A_1 = \frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1}$$

$$A_2 = \frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_0 + Q_1} \ldots\ldots$$

$$A_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} \quad , \text{ for } k \geq 2$$

3.Wiener’s attack on RSA with Gaussian Integer

If the secret exponent d contains at most one-fourth as many bits as the modulus n, a polynomial time approach for cracking a typical (i.e., p and q are gaussian integer of the same size and e < N) RSA cryptosystem has been given. Typically, the Wiener's attack is explained as follows:

If N(P) < N(Q) < 2 N(P), e < N and d is the denominator of a convergent of the continued fraction expansion of $\frac{e}{N}$. The basic relationship between exponents serves as the starting point. This means that there is an integer k such that ed – k ø(N)= 1. Now, ø(N) ≈ N implies $\frac{K}{d}$. ≈ $\frac{e}{N}$.. More precisely, we have N − 3 $\sqrt{N}$ < ø(N) < N.

4. The most popular public-key

Shamir, and Adleman, is currently the most widely used public-key cryptographic system. Its security is based on the intractable problem of factoring large numbers. The modulus N of the RSA cipher is the product of two Gaussian integers P and Q. The public exponent e and the secret exponent d are mathematically related, such that $e * d \equiv 1\ (mod\ \varphi\ (\mathcal{N}))$, where $\varphi\ (N) = N(P-1)(Q-1)$. In a typical RSA cipher scheme, P and Q have similar numbers of bits, while e is smaller than $\mathcal{N}$. The encryption and decryption algorithms in RSA are defined as $C = m^e$ mod $\mathcal{N}$ and

$m = C^d$ mod $\mathcal{N}$, respectively.

In 1990, Weiner described a polynomial algorithm for breaking a typical RSA cipher system where P and Q have the same size and e < $\mathcal{N}$, if the secret exponent d has at most one-fourth as many bits as the modulus N.

To improve RSA decryption speed, one might consider using a small secret exponent d. This choice is particularly advantageous in scenarios like communication between a smart card and a larger computer. In this case, it is desirable for the smart card to have a small secret exponent, while the larger computer has a small general exponent to minimize processing requirements on the smart card.

Example 2: Let p = 379, q =239 using Wiener’s attack on RSA with Integer Continued fraction expansion of

Solution:

N = PQ → N = 379×239

N = 90581

ø(N) = (P – 1) (Q – 1) → Ø (N) = 89964

1< e < N → gcd(e , ø(N)) =1→ e =17993

de=1mod $\emptyset$(N) ⟶ d = 17993^{-1}mod 89964 =5

continued fraction:

$\frac{e}{N} = \frac{17993}{90581}$= [0,5, 29,4,1,3,2,4,3].

According to the continued fraction expansion of $\frac{e}{N}$. All convergent $\frac{k}{d}$.

$\frac{k}{d}$= 0, $\frac{1}{5}$, $\frac{29}{146}$, $\frac{117}{589}$, $\frac{146}{735}$, $\frac{555}{2794}$, $\frac{1256}{6323}$, $\frac{5579}{28086}$, $\frac{17993}{90581}$, d = 5

5.Gaussian Integer G[i]

Definition 2.

A gaussian integer is a complex number of the form A + Bi where both A and B are integers. We often denote the set of Gaussian integers by G[i]

Definition 3. NORM

The norm of a Gaussian integers $\alpha = A + Bi$, denote **N** (α) or **N** $(A + B\, i)$ is a real number defined by N $(A + Bi)$ = $(A + Bi)$ $(A - Bi)$ = A^2+ B^2

The Euclidean Algorithm 4:

A greatest comm divisor (gcd) of P and Q is P common divisor with maximum norm P, Q∈ G [i] and P, Q are non-zero.

Theorem (Euclid’s algorithm).

Let P, Q ∈ G [i] be non-zero. Recursively apply the division theorem, starting with this pair, and make the divisor and remainder in one equation the new dividend and divisor in the next, provided the remainder is not zero:

$P = Q\gamma_1 + \rho_1$, $N(\rho_1) < N(Q)$

$Q = \rho_1\gamma_2 + \rho_2$, $N(\rho_2) < N(\rho_1)$

$\rho_1 = \rho_2\gamma 3 + \rho_3$, $N(\rho_3) < N(\rho_2)$ . . .

The last non-zero remainder is divisible by all common divisors of P and Q, and is itself a common divisor, so it is a greatest common divisor of P and Q.

Euler’s congruence in G [i] 5:

for non-zero P in G [i] , set ø(P) = $\left|\left({}^{G\ [i]}/_{p}\right)x\right|$ When P = π is prime , every non-zero gaussian integer modulo π is invertible ,so ø(P) = N(P) – 1

6. The RSA Algorithm on Gaussian Integer G$[i]$:

Key Generation

1- Select P, Q where P & Q both prime, P ≠Qin Z$[i]$, prime (4K + 3)
2- Calculate N = N (P) N(Q)
3- Calculate ø(N) = (N(P)-1) (N(Q)-1)
4- Select integer e such that gcd(Ø(N), e) =1; 1< e < Ø(N)
5- Calculate d = e^{-1}mod Ø(N)
6- public key: PU= $\{e, N\}$
7- private key PR = $\{d, N\}$

Encryption: C = M^e mod N, Decryption: M = C^d mod N

1.Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
integer	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Gaussin integer	1	1+i	3	2i	1+2i	6	7	2+2i	3i	10	11	12	2+3i	14	15	4i

Q	R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25	26
1+4i	3+3i	19	20	21	22	23	24	5i	1+5i

6. Proposed method:

In this section, we propose a new type of Wiener paired RSA attack modification that operates in the domain of integers. Since it is converted to a gaussian integer after finding the appropriate starting asymptote, this new continuous fraction is also used for trace estimates from encoding and decoding massages.

Example 3. Perform Encryption and Decryption using Wiener's attack on RSA with Gaussian Integer p = 3, q =3+2i massage: KWATT

Solution:

N(P) < N(Q) < 2 N(P)

N = N(P)N(Q) → N = N(3)N(3+2i)

N = 9×13=117

Ø(N)= (N(P) – 1 N(Q) – 1) → Ø(N)ϕ(N) = 96

1< e < N → gcd(e , Ø(N)) =1→ e =55

de=1mod Ø(N)→ d = 55^{-1}mod 96 = 7

continued fraction:

$\frac{e}{N} = \frac{55}{117} =$ [0,2, 7,1,6].

Convergent: $A_0 = \frac{P_0}{Q_0} = 0$, $A_1 = \frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{2(0)+1}{2} = \frac{1}{2}$

$A_2 = \frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_0 + Q_1} = \frac{7}{15}$

$A_3 = \frac{8}{17}$, $A_4 = \frac{117}{55}$

$\frac{K}{d} = [0,\ 2,\ \frac{15}{7}, \frac{17}{8}, \frac{117}{55}]$].→ $\frac{K}{d} = \frac{15}{7}$

Massage: KWATT

Encryption: $C = M^e$ mod N

$C_1 = 11^{55}$mod117 =2

$C_2 = 23^{55}$mod 117 = 23

$C_3 = 1^{55}$mod 117 = 1

$C_4 = 20^{55}$mod117 = 110

$C_5 = 20^{55}$mod117 = 110

Decryption: M= C^{d} mod N

$M_1 = 2^7$ mod 117 =11

$M_2 = 23^7$mod117 = 23

M_3= 1^7mod 117 = 1

M_4= 110^7mod117 = 20

M_4= 110^7mod117 = 20

Example 4. Perform Encryption and Decryption using Wiener’s attack on RSA with Gaussian Integer p = 1+i, q =1+4i massage: STEVEN

Solution:

N = N(P)N(Q) → N = N(1+i) N(1+4i)

N = 34

Ø(N)= (N(P) – 1 N(Q) – 1) → Ø(N)= 16

1< e < N → gcd (e, Ø(N)) =1→ e =13

de=1mod Ø(N)→ d = 13^{-1}mod 16 = 5

continued fraction:

$\frac{e}{N} = \frac{13}{34}$= [0,2, 1,1,1,1,2].

Convergent:

$A_0 = \frac{P_0}{Q_0} = 0$

$A_1 = \frac{P_1}{Q_1} = \frac{q_0 q_1+1}{q_1} = \frac{0(2)+1}{2} = \frac{1}{2}$

$A_2 = \frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_0 + Q_1} = \frac{1}{3}$

$A_3 = \frac{2}{5}$, $A_4 = \frac{3}{8}$, $A_5 = \frac{5}{13}$, $A_6 = \frac{13}{34}$

$\frac{K}{d} = [0,2, 3, \frac{5}{2}, \frac{8}{3}, \frac{13}{5}, \frac{34}{13}]. \rightarrow \frac{K}{d} = \frac{13}{5}$

Massage: STEVEN

Encryption: C = M^e mod N

C_1=19^{13}mod 34=15

C_2 = 20^{13}mod 34 = 12

C_3= $(1+ i)^{13}$mod 34 = (1+6 i)

$C_4 = 22^{13} \text{mod} 34 = 20$

$C_5 = (1 + i)^{13} \text{mod } 34 = (1+6\ i)$

Decryption: $M = C^{\ d} \text{mod } N$

$M_1 = 15^5 \text{ mod } 34 = 19$

$M_2 = 12^5 \text{mod } 34 = 20$

$M_3 = (1+6\ i)^5 \text{mod } 34 = (1+ i)$

$M_4 = 20^5 \text{mod} 34 = 22$

$M_5 = (\ 1+6\ i)^5 \text{mod } 34 = (1+ i)$

Example 5. Perform Encryption and Decryption using Wiener’s attack on RSA with Gaussian Integer P= 1+2i , Q= 2+3i massage: BIRD
Solution:

$N = N(P)N(Q) \ \rightarrow N = N(1+2i)N(2+3i)$

$N = 5 \times 13 = 65$

$\text{Ø}(N) = (N(P) - 1\ N(Q) - 1) \rightarrow \text{Ø}(N) = 48$

$1 < e < N \rightarrow \gcd(e\ ,\ \phi(N)) = 1 \rightarrow e = 7$

$de = 1 \text{mod } \text{Ø}(N) \rightarrow d = 7^{-1} \text{mod } 48 = 7$

continued fraction:

$\frac{e}{N} = \frac{7}{65} = [0,9,\ 3,2].$

Convergent:

$A_0 = \frac{P_0}{Q_0} \ = 0$

$A_1 = \frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1} = \frac{0(9)+1}{9} \ = \frac{1}{9}$

$A_2 = \frac{P_2}{Q_2} \ = \frac{q_2 P_1 + P_0}{q_2 Q_0 + Q_1} = \frac{3}{28}$

$A_3 = \frac{7}{65}$

$\frac{K}{d} = [0,9, \frac{28}{3}, \frac{65}{7}]. \rightarrow \frac{K}{d} = \frac{65}{7}$

Massage: BIRD

Encryption: $C = M^e \bmod N$

$C_1=(1 + i)^7 \bmod 65 = 8 – 8i$

$C_2 = (3i)^7 \mathrm{mod}65 = 42i$

$C_3= (3+3i)^7 \mathrm{mod}65 =11-11i$

$C_4= (2i)^7 \mathrm{mod}65 = 2i$

Decryption: $M= C^d \bmod N$

$M_1= (8 – 8i)^7 \bmod 65 = 1 + i$

$M_2 = (42i)\ 7\mathrm{mod}72 = 3i$

$M_3= (11-11i)^7 \bmod 65 =3+3i$

$M_4= (2i)^7\mathrm{mod}65 = 2i$

Conclusion

Through the results above within attack RSA defined on the Gaussian integer in a way continued fraction by modifying Wiener’s attack The modified method has proven effective in attacking the algorithm's encryption system RSA on gaussian integer

References

1. William Stallings, Cryptography and Network Security, 1999.
2. KHINCHIN, A. Ya.: Continued Fractions, Dover, New York, 1997
3. J¨orn Steuding. Diophantine Analysis. Chapman and Hall/CRC. 2005.
4. LANG, S.: Introduction to Diophantine Approximations, Addison-Wesley, Reading, 1966.
5. Rana Bassam Badawi, On Continued Fractions and its Applications An-Najah National University, Nablus, Palestine. 2016
6. HINEK, M. J.: Low Public Exponent Partial Key and Low Private Exponent Attack's on Multi-prime RSA, Master’s thesis, University of Waterloo, 2002.