Proceedings of the 2023 International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/11/20230367

Development of RSA and some attack points

Xurui Zhang

SanJiang University Nanjing China 225741 310 Longxi Road, Yuhuatai District

sr555498@163.com

Abstract. Currently, the relatively popular public key encryption is RSA. It was officially launched in 1978 and given their initials as a name. Different encryption and decryption keys are used in the RSA public-key cryptosystem. Deriving decryption keys from known encryption keys is computationally difficult. Rsa has emerged in various forms since its development. Since the development of RSA, there have been various forms, which means there are various loopholes. Next, we will summarize several interesting attack methods of rsa. It will involve continued fractions and CRT and so on. Through this paper, one can learn a series of knowledge about rsa. As a classic asymmetric password, the value of rsa's existence is relatively high, and exploring its value is something that every password learner should experience. Through this article, one will learn about the most basic attack methods of rsa.

Keywords: CRT, RSA, continued fractions.

1. Introduction

RSA algorithm is developed on the basis of number theory, and number theory - or some people call it arithmetic - is the oldest, purest, most energetic, original and most profound mathematical field. It is no accident that this subject has the reputation of "queen of mathematics". Some of the most complex traditional mathematical ideas are developed from the study of the basic problems of logarithmic theory. As early as in the ancient Greek era, people began to obsessively study numbers and immerse themselves in this thinking game with little practical value. Until the birth of the computer, the research results of number theory for thousands of years suddenly had practical applications. This process can be said to be one of the most exciting mathematical topics.

RSA algorithm is the product of that era and has an absolute position in cryptography. It is worth every person's careful study and understanding. The knowledge of number theory and asymmetry in rsa also has great learning value, and it is applicable as the first stop for learning public key encryption.

This article will describe RSA's attack tactics under CRT and continuous fraction, and will describe the definition of continuous fraction and CRT. There are many interesting and meaningful knowledge in it, and learning the knowledge will provide great help in understanding rsa

First of all, we need to know RSA encryption process.

DOI: 10.54254/2753-8818/11/20230367

2. RSA encryption

2.1. Generation of public and private keys

Suppose Alice wants Bob's confidential message over an untrustworthy medium. The process is illustrated as follows.

You can freely choose two large prime numbers, which are p and q, calculate n=p*q.

According to the Euler function, the quantity of positive integers fewer than n that are also prime has the formula:

$$N = phi(n) = (p-1) * (q-1) \tag{1}$$

Select an integer e and phi (N), and e is less than phi (N).

To determine d, use the following formula: e * d=1. Modifying phi (N) When the extended Euclidean algorithm is used to calculate e, the result is (d), which is the inverse of modulo phi (N) of e.

p and q's records should be destroyed because it will be very challenging to find them if N is large enough.

The private key is (d, N), while the public key is (e, N). (d, N) is not public. Bob receives Alice's public key (e, N), but Alice conceals her private key (d, N).

2.2. Encryption process

Suppose A wants to send B a message M. He is aware of B's produced public key (e, N). A transforms M into an integer n smaller than N using the format already agreed upon with B. For instance, he could turn each character into a number representing its Unicode code, then join those numbers to create the integer n (if his data is particularly lengthy, he could break it up into multiple segments and encrypt each separately). The following congruence formula is used by public key (e, N) to encrypt n into C.

$$C = M^e \bmod N \tag{2}$$

2.3. Decryption process

Alice decodes Bob's message C using her private key (d, N). Alice can apply the following congruence formula to convert C to m

$$M = C^d \bmod N \tag{3}$$

3. Prerequisite knowledge

3.1. CRT

Theorem. In n = p*q, let p and q be different primes. For any pair (x1, x2) where 0<x1<p and 0<x2<q, there is a single number x, where 0 × N makes x1=x mod p and x2=x mod q. The original name of CRT is the Chinese remainder theorem. This is the case in detail

The Chinese remainder theorem gives the following linear congruence equations of one variable

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$x \equiv a_3 \bmod m_3$$

We make

$$M = m_1 * m_2 * m_3$$
$$M_i = M/m_i \quad M_i * t_i = 1 \bmod m_i \tag{4}$$
$$\text{so } x = \left(\sum_{i=1}^{n} a_i t_i M_i\right) \bmod M \tag{5}$$

3.2. Continuous fraction

Here, we only need to understand the asymptotic continuous fraction and the continuous fraction transformation law. In fact, it is monotonicity research.

$$x_m - x_{m-2} = \frac{p_m}{q_m} - \frac{p_{m-2}}{q_{m-2}}$$

DOI: 10.54254/2753-8818/11/20230367

$$= \frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}} + \frac{p_{m-1}}{q_{m-1}} - \frac{p_{m-2}}{q_{m-2}}$$
$$= \frac{(-1)^{m-1}}{q_m q_{m-1}} + \frac{(-1)^{m-2}}{q_{(m-1)q_{m-2}}}$$
$$= \frac{(-1)^m (q_m - q_{m-2})}{q_m q_{m-1}\, q_{m-2}}$$
$$= \frac{(-1)^m a_m q_{m-1}}{q_m q_{m-2} q_{m-1}}$$
$$= \frac{(-1)^m a_m}{q_m q_{m-2}}$$

Figure 1. Calculation of monotonicity of continued fractions [1].

This also means that the continuous score and its upper limit can be expanded continuously. Generally, the maximum probability of RSA using its method to expand the probability is 1.

4. CRT-RSA

This acceleration supports the usage of CRT-RSA whenever N's factorization and p q is known. The private key in CRT-RSA is a 5-tuple (p, q, dp, dq, iq), whose structure is more diverse than just (N, d) [2].

$$\mathrm{d_p} = \mathrm{dmod(p-1)}$$
$$\mathrm{d_q} = \mathrm{dmod(q-1)}$$
$$\mathrm{i_q} = \mathrm{d^{-1}modp} \quad (6)$$

Algorithm 1: Unprotected CRT-RSA

$$input: Message\ m\ , key(p, q, d_p, d_q, i_q)$$

$$output: Signature\ m^d mod N$$

$$S_p = m^{d_p} mod\ p$$

$$S_q = m^{d_q} mod\ q$$

$$S = S_q + q * (i_q * (S_p - S_q) mod\ p)$$

Return

Figure 2. CTR-RSA [2].

4.1. How to solve simple CRT-RSA

First we know $\mathrm{c = m^e modn}$, and $\mathrm{m = c^d modn}$,may be we can get like this

$$\mathrm{m_1 = c^d modp} \quad (7)$$
$$\mathrm{m_2 = c^d modq} \quad (8)$$

Also we can get $\mathrm{d * e = 1 mod\varphi(n)}$

So we get a $\mathrm{m_1}$, so we can make this equation

$$\mathrm{d = k * \varphi(p) + d\ mod\varphi(p)}$$

So $\mathrm{m1 = c^d modp = c^{k\varphi(p)+d\ mod\ \varphi(p)}\ mod\ p = \left(c^{\varphi(p)}\right)^k * c^{dmod\varphi(p)}\ mod\ p = 1^k * c^{dmod\varphi(p)}\ modp}$

The transformation borrows Euler formula

Just like this

$$\mathrm{c^{\varphi(p)} = 1\ mod\ p}$$

DOI: 10.54254/2753-8818/11/20230367

The change of m_2 is the same as the change of y above

$$d_p = d \bmod (p-1)$$
$$d_q = d \bmod (q-1)$$

So we get new equations

$$m_1 = c^{dp} \bmod p$$
$$m_2 = c^{dq} \bmod q$$

At this point, the equation form of CRT is satisfied, so the problems of RSA is tackled.

Then, we retrieve m by applying Garner's method to our previously computed qInv.

$$qInv = q^{-1} \bmod p$$
$$h = qInv * (m_1 - m_2) \bmod p$$
$$m = m_2 + h * q$$

m is the clear text that is needed.

We can take a value to do a test.

p = 149, q = 197, n = 137.131 = 29353, e = 3, d = 19339. m = 517

c = 5173 mod n = 23842

m = 2384219339 mod 29353= 517.

Then from the perspective of CRT we need

$$dP = e^{-1} \bmod (p-1) = d \bmod (p-1) = 99$$
$$dQ = e^{-1} \bmod (q-1) = d \bmod (q-1) = 131$$
$$qInv = q^{-1} \bmod p = 59$$
$$m1 = c^{dP} \bmod p = 70$$
$$m2 = c^{dQ} \bmod q = 8363^{87} \bmod 131 = 123$$
$$h = qInv * (m1 - m2) \bmod p = 59 * (70 - 123 + 149) \bmod 149 = 2$$
$$m = m2 + h * q = 123 + 2 * 197 = 517.$$

This is the most basic application of CRT-RSA, and other complex applications of CRT-RSA have been written in detail in other senior papers, such as Faults on Montgomery Multiplication [3], This article only recalls the function of Quick Start, and will not elaborate on the difficulties too much.

The known Bellcore attack, which was initially described by Boneh, DeMillo, and Lipton in [4], can compromise RSA-CRT signatures. Here is a brief description of this attack

Three BellCore employees, Boneh, DeMillo, and Lipton [BDL97], made a terrible statement in 1997: If the computation is flawed, even in a highly random fashion, Alg. 1 could betray the hidden primes p and q. This proposition can be used to express the assault.See [2] for further information.

5. Application of continued fractions under RSA

5.1. Wiener's attack on RSA

Wiener's attack uses RSA's global continuous fractions. It represents a famous polynomial-time attack on an RSA cryptosystem with a tiny secret decryption exponent d. It succeeds if d < n0.25, where n = p*q is the modulus. Regarding that scenario, d is the denominator of some convergent pm / qm of the continuous fraction expansion of e/n, so the public key (n, e) can easily compute d.

It applies when N, e is known, and e is too large or too small.

$$\varphi(n) = (p-1) * (q-1) = pq - (p+q) + 1 = N - (p+q) + 1$$

We know p and q are very big, so p*q≫p+q, so we can think that N≈ φ(n)

$$ed \equiv 1 \bmod \varphi(n)$$
$$ed - 1 = k\varphi(n) \quad (9)$$

Divide both sides simultaneously d*φ(n)

$$\frac{e}{\varphi(n)} - \frac{k}{d} = \frac{1}{d\varphi(n)} \quad (10)$$

Just we know N≈ φ(n) ,so

DOI: 10.54254/2753-8818/11/20230367

$$\frac{e}{N} - \frac{k}{d} = \frac{1}{d\varphi(n)} \tag{11}$$

Same d *φ (n) It is a big number, so $\frac{e}{N}$ ls slightly bigger than $\frac{k}{d}$

Because e and N are known, after calculating $\frac{e}{N}$, the $\frac{k}{d}$ slightly smaller than it can be calculated by calculating the continued fraction expansion of $\frac{e}{N}$, and each progressive fraction of this fraction can be calculated in turn. Because $\frac{e}{N}$ is slightly larger than $\frac{k}{d}$, Wiener proved that this attack can accurately cover $\frac{k}{d}$.

It also puts forward restrictions

If p < q < 2p, e < N and d < $\frac{1}{3}\sqrt[4]{n}$, then d represents the denominator of various convergent of the continued fraction expansion of $\frac{e}{N}$ [5].

As soon as d is a longer, Verheul and van Tilborg [6] developed a variant of Wiener's attack that makes it possible to break the RSA cryptosystem. Under plausible assumptions about the underlying partial convergents, their attack for d > is required to conduct a thorough search for roughly 2t+8 bits, where t = log2 (d/).Based on Worley's discovery on Diophantine approximations [7]. This shows that the whole rationals meet the inequality, we presented a small modification of the Verheul and van Tilborg assault in [8].

$$\left|a - \frac{p}{q}\right| < \frac{c}{q^2}, \tag{12}$$

for a positive real number c, it is having the form of:

$$\frac{p}{q} = \frac{r\ p_{\{m+1\}} \pm s p_m}{r\ q_{\{m+1\}} \pm s q_m} \tag{13}$$

Here is also a recursive representation of continued fractions in [1].

Theoretically, in the range from one value to another, if these conditions are met, we can expand to find the number we need.

Similarly, the transformation form

$\frac{N_1}{N_2} < \frac{q_1}{q_2} < 1$ Try to expand $\frac{N_1}{N_2}$ and calculate its progressive fractions, we can also find we need number.

6. Recent developments in RSA

Now RSA is beginning to move towards deeper aspects such as the Lattice protocol. To pursue the problems of SVP and CVP. Therefore, it can be concluded that the development of RSA is continuous. Many RSA problems are also based on the combination of abstract algebra and number theory [9].

RSA will never be outdated, and its development is evolving.

Here the lattice analysis will be explained.

Lattice analysis method stands a fundamental method for analyzing the security of RSA encryption algorithms. The existing standard RSA lattice analysis work can be roughly divided into three categories: modulus decomposition attack, small decryption index attack and partial private key (decryption index) leakage attack. Among them, small decryption index attacks and partial private key disclosure attacks are more complex to attack.

Although the lattice analysis of RSA and its variant algorithms has achieved good results, most of these lattice attacks rely on the parameters of the cryptographic system.

The particularity of number selection or certain requirements on the leakage of private key do not pose a fundamental threat to the practical RSA cryptosystem.

Rational parameters can avoid lattice attacks.

It also shows that its security still exists

DOI: 10.54254/2753-8818/11/20230367

7. Conclusion

This article mainly explains the simple application of CRT and continuous fraction under RSA, and also recommends some deeper understanding methods. It also shows the scalability and security of RSA. This can also explain why RSA often appears in various competitions. In my opinion, as a great ancestor of public key cryptography, its historical position is always very important.

Finally, in my opinion, the emergence of RSA attack points also shows that there is no absolute security. Only by leaving no attack points can a good encryption be completed.

This paper has limitations. Attacks can only be applied to attacks that can satisfy conditions, and divergence needs to be discussed

References

[1] Gautam Gopal Krishnan(2016) Continued Fractions.

[2] Rauz, P. and Guilley, S. (2014) A Formal Proof of Countermeasures Against Fault Injection Attacks on CRT-RSA. Available at: https://eprint.iacr.org/2013/506.pdf .

[3] Fouqu, P.-A., Guillermi, N. and Leresteu, elphine (no date) Attacking RSA{CRT signatures with faults on Montgomery multiplication, Attacking RSA–CRT Signatures with Faults on Montgomery Multiplica. Available at: https://eprint.iacr.org/2012/172.pdf (Accessed: March 15, 2023).

[4] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults. In EUROCRYPT, pages 37–51, 1997.

[5] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In Proceedings of Eurocrypt'97, volume 1233 of LNCS, pages 37–51. Springer, May 11-15 1997. Konstanz, Germany. DOI: 10.1007/3-540-69053-0 4

[6] Dujella, A. (no date) A variant of Wiener's attack on RSA - eprint.iacr.org, A variant of Wiener's attack on R. Available at: https://eprint.iacr.org/2008/459.pdf (Accessed: March 15, 2023).

[7] E. R. Verheul, H. C. A. van Tilborg, Cryptanalysis of 'less short' RSA secret exponents, Appl. Algebra Engrg. Comm. Computing 8 (1997), 425–435.

[8] R. T. Worley, Estimating $|\alpha - p/q|$, Austral. Math. Soc. Ser. A 31 (1981), 202–206.

[9] A. Dujella, Continued fractions and RSA with small secret exponent, Tatra Mt. Math. Publ. 29 (2004), 101–112.

Acknowledgement

The research was completed under the careful guidance of the teacher and my own efforts. This teacher's profound professional knowledge, rigorous academic attitude, continuous improvement work style, tireless noble professional ethics, strict discipline and broad mindedness, and simple and approachable personality charm have had an impact on me. Moreover, I have learned many methods of dealing with people and the spirit of research.