Serious Security Weakness in RSA Cryptosystem

Majid Bakhtiari [1] Mohd Aizaini Maarof [2]

**[1] Department of Computer Science & Information Systems, University Technology Malaysia,
Skudai Johor Bahru, 81310, MALAYSIA**

**[2] Department of Computer Science & Information Systems, University Technology Malaysia,
Skudai Johor Bahru, 81310 MALAYSIA,**

Abstract

Nowadays, RSA is the well-known cryptosystem which supports most of electronic commercial communications. RSA is working on the base of multiplication of two prime numbers. Currently different kinds of attacks have indentified against RSA by cryptanalysis. This paper has shown that regardless to the size of secret key and public key, it is possible to decrypt one cipher text by different secret keys RSA algorithm and in excellent condition, there are two similar key at least available in domain of two prime numbers multiplication.

Keywords: *RSA, Similar Key, Different Secret Key, Encryption, cryptanalysis.*

1. Introduction

RSA algorithm has invented by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) in 1977 [1]. RSA has categorized in asymmetric key classification and it has capability to supports encryption and digital signature [2].

Currently, RSA is used in security protocols [3] such as:

- TLS/SSL - transport data security (web)
- PGP - email security
- IPSEC/IKE - IP data security
- SILC - conferencing service security
- SSH - terminal connection security

Nevertheless, the RSA is a famous public key algorithm used in the world.

RSA is working on the base of multiplication of two prime numbers. Therefore, number factorization is a serious threatening against RSA. Today, the large numbers factorization is major problem in the world. However, there are a lot of inefficient algorithms available today which will correctly factor big numbers. The idea of RSA can be best depicted in Figure 1.

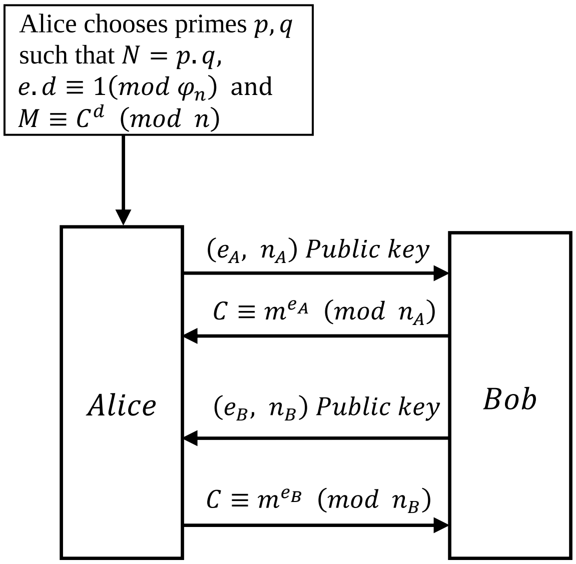
Alice chooses primes p, q such that $N = p.q$, $e.d \equiv 1(mod\ \varphi_n)$ and $M \equiv C^d\ (mod\ n)$
$Alice$
Bob
$(e_A,\ n_A)\ Public\ key$
$C \equiv m^{e_A}\ (mod\ n_A)$
$(e_B,\ n_B)\ Public\ key$
$C \equiv m^{e_B}\ (mod\ n_B)$

Fig. 1: Diagram of RSA Encryption and Decryption

With consider that RSA cryptosystem works on a given modulus "n" that is the product of two prime random numbers "p" and "q", a public exponent "e", and an element $C \in Z_n$, users find "m" such that $C = m^e\ mod\ n$ and a private exponent "d" that should satisfy $m = C^d\ mod\ n$. Therefore, at the first view the following items should be considered:

- The bit-size of "n"
- The size of the public exponent "e"
- The size of the private exponent "d"
- The factorization of "n"
- The features of two big random prime numbers

In 1977 Ron Rivest said that factoring a 125-digit number would take 40 quadrillion years. In 1994 RSA129 was factored using about 5000 MIPS-years of effort from idle CPU cycles on computers across the Internet for eight months. Today, it is possible to factorize 192 digit numbers easily [4].

However, there are some algorithms namely the Trial division, Pollard's Rho algorithm, Pollard's p-1 algorithm, Williams' p+1 algorithm, Lenstra elliptic curve factorization, Fermat's factorization method and Special number field Sieve that can factorize big numbers into prime numbers. But this paper concentrates on the other viewpoint in RSA which explore one of the big weaknesses of RSA cryptosystem.

This paper has shown that regardless to the size of secret key and public key, it is possible to decrypt one cipher text in RSA algorithm by different secret keys.

2. Background

There are many kinds of attacks have known against RSA algorithm. The most well-known of them are listed as follows:

- Common modulus
- Blinding
- Small encryption exponent "e"
- Small decryption exponent "d"
- Forward search attack
- Timing attack
- Multiplicative properties
- Cycling attack
- Message concealing
- Faulty encryption attack
- Factoring the public key

It should be notice that no attack algorithm can break RSA cryptosystem in efficient manner. Most attacks appear to be the result of misuse of the system or bad choice of parameters. Analysis of the known attacks shows that RSA has not been proven to be unbreakable, but having survived a great deal of cryptanalytic security over the last thirty years [5].

3. New Security Weakness in RSA

According to Fermat's little Theorem on the probable prime number which stated if p is a prime and a is an integer coprime to p, then $a^{p-1} - 1$ will be evenly divisible by p. Therefore, in the notation of modular arithmetic:

$a^{p-1} \equiv 1 \; mod \; p$. Otherwise, p is composite number.

With consider that RSA algorithm is working on the base of two prime numbers p, q. The Fermat's theory can be expanded in some part of RSA algorithm as follows:

$$n = p.q$$
$$\varphi = (p-1)(q-1)$$
$$2^{p-1} \; mod \; p = 1 \qquad (1)$$
$$2^{q-1} \; mod \; q = 1 \qquad (2)$$

From Eq. 1 and Eq. 2:

$$2^{\varphi} mod \; n = 1 \qquad (3)$$

On the other hand, with consider that $(p-1)$ and $(q-1)$ are dividable to 2, therefore, in second step:

$$2^{\frac{\varphi}{2}} mod \; n = 1 \qquad (4)$$

Eq. 4 is proving that, at least it is two same fields available between 0 to n. In other word

$$2^{\varphi+\Delta x} \; mod \; n = 2^{\frac{\varphi}{2}+\Delta x} \; mod \; n \qquad (5)$$

Eq. 5 is proving that at least two same fields are available in domain of "n". It means that any number between $1 \; to \; \frac{\varphi}{2}$ have same properties to any number between $\frac{\varphi}{2} \; to \; \varphi$. With consider that "$e$", "$n$" as public key and "$d$" ,"$n$" as secret key have located in domain of $\frac{\varphi}{2}$.

Therefore, as it has shown in Figure 2, there are at least two "d" and two "e" are available which have exactly same properties concerning to RSA cryptography operations.

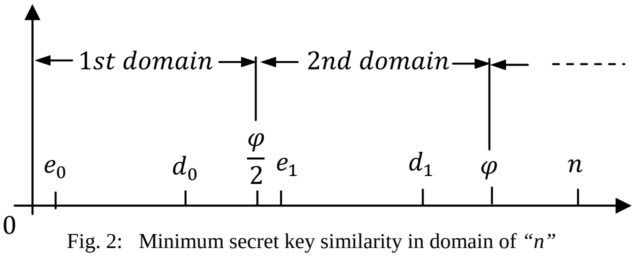

Fig. 2: Minimum secret key similarity in domain of "n"

$$C = m^{e_0} \; (mod \; n) = m^{e_1} \; (mod \; n) \qquad (6)$$
$$m = C^{d_0} \; (mod \; n) = C^{d_1} \; (mod \; n) \qquad (7)$$

As it has shown in Eq. 6 and Eq. 7, it is possible to decrypt one cipher text by two separate secret keys. It should be noticed that the Eq. 6 and Eq. 7 are valid if and only if that two prime numbers (p, q) have unique specification. Otherwise, the numbers of secret keys which can decrypt one cipher text are more than two in domain of "n". The unique specification of two prime numbers have identified as follows:

- $\frac{p-1}{2}$ must be prime number.
- $\frac{q-1}{2}$ must be prime number.

Those numbers which have passed above condition successfully called “strong prime” in this paper. If and only if, *p*, *q* cannot pass the strong prime conditions successfully, the number of similar secret keys (which are more than two keys) are depend to combination of factorization items of *p* and *q*. The following example shows one sample of this procedure, if *p* and *q* cannot pass above condition successfully.

$$p = 401 \quad ; \quad q = 281 \quad ; \quad n = 112681 \quad ; \quad e = 3$$

$$p - 1 = 2^4 * 5^2$$
$$q - 1 = 2^3 * 5 * 7$$

With consider that, public key and secret key should be generated on the base of φ. Therefore, selected prime numbers (*p*, *q*) have 40 secret key that each one can decrypt all of cipher texts that encrypted by one public key. It is because $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are not prime number. In this example, Table 1 shows some of same secret keys for a public key $(3, 112681)$.

Table 1: One public key with different similar secret keys (*n=112681*)

Public Key	Secret key
$e = 3$	$1867, 4667, 27067, \ldots$

It is important to notice that finding *p* and *q* in such a way that $p \pm 1$ and $q \pm 1$ to have large prime factor are not enough conditions that RSA laboratories advised [6-8]. It is because; mentioned conditions cannot solve similarity keys in domain of “*n*”. They tried just to reduce this serious weakness in RSA.

On the other hand, it should be mention that the numbers of strong prime numbers are very limited. According to study that generated Figure 3, number of strong prime numbers for more than 256 bits (77 digits) are very limited. Therefore, most of pair prime numbers cannot provide the defined condition. Also this why that RSA laboratory advise to select large prime numbers with large prime factor [7].

Figure 3 shows the density of strong prime numbers up to 20 digits (64-bit). As it has shown, they are very limited and it is possible to generate those numbers and store them in one data base centre for efficient attack against RSA.

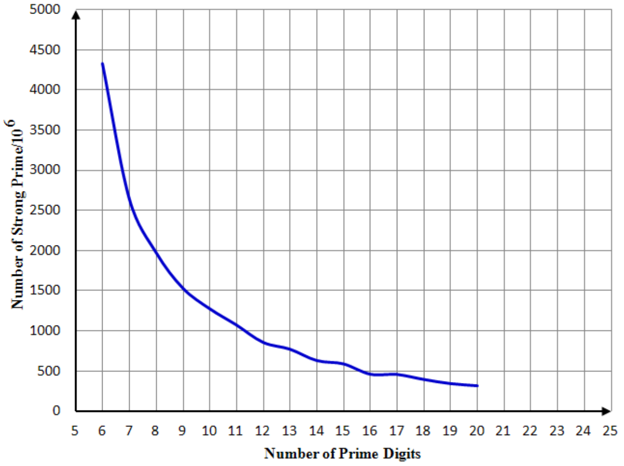

Fig. 3: The density of strong prime numbers for RSA

3.1 Number of similar secret key

By extending the properties of two prime numbers multiplication which RSA cryptosystem is following, there are many similar secret keys are available out of domain of “n”. It means that even by selecting strong prime numbers, there are infinite secret keys exist which located in $\mathbb{R}$. The distance of each secret key that has shown in Figure 4 is equal to $LCM\big((p-1),(q-1)\big)$.

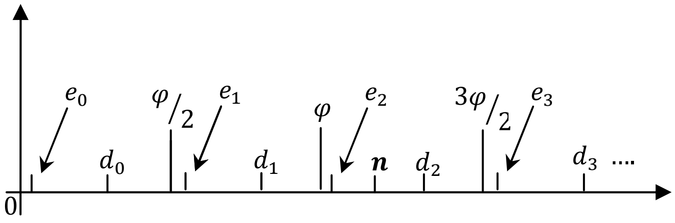

Fig 4: Number of similar secret keys in Real Number field

Figure 4 shows that there are infinite “*d*” are available which can decrypt a massage that encrypted by $e_i \;\; ; \;\; i > 0$. It means that for $C_1 = m^{e_i} \, mod \, n \;\; ; \;\; i > 0$, it is possible to find plain message by $m = C_1^{d_j} \, mod \, n \;\; ; \;\; j > 0$. The minimum distance between two secret key is equal to $d_{i+1} - d_i = LCM\big((p-1),(q-1)\big) \quad ; \quad i \geq 0$.

3.2 New threatening on RSA

According to discussion in Section 3 by Eq. 5, due to structure of RSA which has based on multiplication of two prime numbers, there is new vulnerability available in RSA; even two prime numbers are strong prime. As it has shown in following equation:

$$p = k.q \qquad \Longrightarrow \qquad n = k.q^2 \qquad (8)$$

$$\sqrt{n} = q\sqrt{k} \qquad \Longrightarrow \qquad \begin{cases} q\sqrt{k} < p \\ q\sqrt{k} > q \\ q\sqrt{k} < \frac{p+q}{2} \end{cases} \qquad (9)$$

$$\text{From Eq. 9} \Longrightarrow \frac{p+q}{2} - \Delta x = q\sqrt{k} \qquad (10)$$

Therefore,

$$2^{(n-q\sqrt{k})} \ \ mod \ \ n = 2^{\left(\frac{p+q}{2}+\Delta x\right)} \ mod \ \ n \qquad (11)$$

In this step, it is important to find one feature from point of $\frac{p+q}{2}$. According to Eq. 3 and Eq. 4, we can write Eq. 12 as follow:

$$2^{\frac{n+1}{2}} \, mod \, n = 2^{\frac{p+q}{2}} \ mod \, n \qquad (12)$$

With consider that, the left side of both Eq. 12 and Eq. 11 are determined and right side of Eq. 10 is determined too. Therefore, it is concluded that the maximum security level for RSA is equal to find Δx. while Δx is very smaller than amount of "q". However, there are different methods are available to find Δx.

Figure 5 shows a sample flow diagram to finding Δx. In method which has shown in Figure5, basic instruction are just shift left ($x = x * 2$), take modulo n and simple addition. However, there are different methods exist to find $LCM(p-1, q-1)$ by Eq. 12.

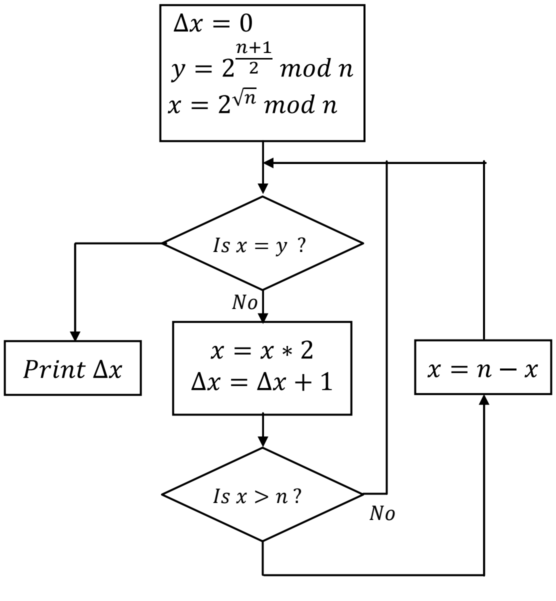

Fig. 5: One sample flow diagram to finding Δx

4. Conclusion and Future work

This paper proved that RSA cryptosystem has at least two similar secret key in domain of "n" for all of cipher texts and infinite similar secret key are exist out of domain of "n". Also this paper proved that the maximum security level of RSA is not equal to bit-length of "n" and for any length-bit of "p" and "q". According to study of this paper, the security level of RSA cryptosystem is smaller from digit length in comparison to each of two selected prime numbers.

Currently, it is not correct evaluation between different cryptosystem and RSA. Finding an efficient method to obtain Δx or φ_n by Eq. 12, and then evaluating RSA cryptosystem from security level view point can be good future work to evaluate RSA cryptosystem.

References

[1] Rivest, R.L., A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 1978. **21**(2): p. 120-126.

[2] ElGamal, T. *A public key cryptosystem and a signature scheme based on discrete logarithms*. 1985: Springer.

[3] Sonsare, P.M. and S. Sapkal. *Stegano-CryptoSystem for Enhancing Biometric-Feature Security with RSA*. 2011.

[4] Cavallar, S., *et al. Factorization of a 512-bit RSA modulus*. 2000: Springer.

[5] Salah, I.K., A. Darwish, and S. Oqeili, *Mathematical attacks on RSA cryptosystem*. Journal of Computer Science, 2006. **2**(8): p. 665-671.

[6] Rivest, R. and R.D. Silverman. *Arestrong'primes needed for RSA,"*. 1997: Citeseer.

[7] Silverman, R.D., *Fast generation of random, strong RSA primes*. CryptoBytes, 1997. **3**(1): p. 9-13.

[8] Gordon, J., *Strong RSA keys*. Electronics Letters Published by IEEE, 1984. **20**(12): p. 514-516.