Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 1340 – 1344

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Analysis of RSA based on Quantitating Key Security Strength

Wenxue Tan [a], Xiping Wang [b], Xiaoping Lou [c] and Meisen Pan [d] a*

[a c d] *College of Computer Science and Technology, Hunan University of Arts and Science, Changde 415000, P.R. China*
[b] *College of Economy and Management, Hunan University of Arts and Science, Changde 415000, P.R. China*

Abstract

RSA is an asymmetric crypto algorithm which is applied widely in the information security of E-Commerce and Internet-Bank. Its security has been withstanding tests since several decades ago. But the key security isn't equal to that of algorithm, which is often neglected by most of users and scholars. As to most constructions, they lack definite recognition to the safety of the RSA key. As a result, even some strong crypto-algorithms used it still meets the security predicament. In this paper, start with the known plaintext attack to RSA public key crypto scheme, we pioneer the mechanism of quantitation of the RSA key security strength, the concept of key security coefficient, the evaluation model of security coefficient and the algorithm to extract security strength. Further more, an innovative method of generating secure keys is proposed. After some experimentations, the security performance of key and distribution of secure key-amount, and their key security coefficient are surveyed and analyzed in detail. The theoretic analysis and statistics demonstrate that our mechanism could elevate security of RSA in effect.

Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: cryptography analysis; key security strength; threshold of security ;security quantitation; secure key.

1. Introduction

RSA is a public key algorithm which has been being applied extensively in the area of information security because of its concise preliminary , believable security and understandability [1].Many attack algorithms against RSA are reduced to the attack against IFP in mathematical essence, yet, none of which

* Corresponding author.
E-mail address:twxpaper@163.com.

doi:10.1016/j.proeng.2011.08.248

presents a satisfying effect. In addition, because of either the defects or shortcomings of RSA exposed when it being implemented other attack means could attack effectively RSA in some especial case. For example, chosen cipher-text attack, public modulus attack and low encryption exponent attack, and so on. However, there is no universal and effective crack algorithm hitherto [2].

The attack to RSA becomes a research hot of applied cryptograph area, and the method of known plaintext attack comes into the sight of scholars. For instance, u=6973, p=107, q=167, n=17869, *plaintext*=12345, if repeat the RSA encryption operation 4 times, and the *plaintext* is restored. “4 times” be equivalent to a second secret private key discovered by the third party, which makes it very easy to inform the hacker of the private information sent by sender.

Is this case the result of either the RSA algorithm itself or the overlook in the generation of RSA keys ? Herein, we start an extensive and in-depth exploration in order to perfect RSA crypto scheme.

2. Analysis of Chosen Cipher-text Attack against RSA

RSA algorithm consists of 3 steps which include key-pair extraction, block encryption and decryption. The mathematical proof of RSA is demonstrated in detail in [2]. “Don’t factor n and calculate the u-th root modulus n” is a well known difficult problem, even against the background of strong computability today. If choose n with enough bits at length, that still is a computationally infeasible problem [3,4]. If it is proved to be true that any method to break RSA maybe educe an effective algorithm to factor big integer, we can draw a conclusion that breaking RSA and integer-factor-problem are with the same degree difficulty. However, it is even a unable confirmed hypothesis. In view of “ p-1 factoring method ”, p and q are subject to that both p-1 and q-1 should contain enough big prime factors. Conventional process is to select two big primes p_1 and q_1, subject to p=2p_1+1, q=2q_1+1 to be another pair primes, which named strong primes or secure primes .

$$\mathrm{Q}\; u^{r} \equiv 1 \bmod (p-1)(q-1), \gcd(u,(p-1)(q-1)) = 1.$$

$$\therefore u^{\varphi[(p-1)(q-1)]} \equiv 1 \bmod (p-1)(q-1), r \equiv u^{\varphi[(p-1)(q-1)]-1} \bmod (p-1)(q-1).$$

By operating u with limited times modulus exponential operation ,denoted by a times, it is easy to find the secret exponential index r, Φ[(p-1)(q-1)]-1 times are sure to succeed. Does there exist a smaller number than Φ[(p-1)(q-1)]-1 to succeed ? Facts demonstrate that Φ[(p-1)(q-1)]-1 times only form a sufficient condition, not necessary. Known a cipher-text M_0,$M_0^u \equiv M_1 \bmod n$; $M_1^u = M_2 \bmod n$, $\cdots M_i^u = M_{i+1} \bmod n$. If M_i= M_0 then find $a = i$, the process above can be integrated as $(M_0^u)^i \equiv M_0 \bmod n$.

That is to say $u^{(i-1)} = r \bmod (p-1)(q-1)$. If encrypt plaintext for some times, you will get the same plaintext. Such as the example referred in the foreword, u = 6973, p = 107, q = 167, n= 17869, (p-1)×(q-1) =17596, i=a=4, $u^3 \equiv 15605 \bmod 17596$. This method is much easier to attack RSA than factoring n, and the keys as it are insecure [5,6].

3. Preliminaries of Key Security Quantitating

3.1. Definition 1 :Key Security Strength

Given two strong primes *p* ***and*** *q*, ***along with an integer*** *u* ***subject to*** *GCD*(u,(p-1)(q-1))=1, ***if there exists the least positive integer denoted by*** *s* ***to hold the condition*** $u^s \equiv 1 \bmod (p-1)(q-1)$,***then define*** *s* ***as the*** *key security strength* of ***the key*** (u, pq).

According to the analysis mentioned above ,when selecting different prime pair of p and q, the key-strength varies in a larger scale. For example, as to (59,83), the security strength s_{max} is 280,and there are

786 keys reaching this strength, the distribution is discontinuous. In general, along with the increment of strength and the number of responding keys increasing [7,8].

3.2. Definition 2: Collection of Secure Keys

Given two strong primes** p **and** q, **define the** collection of secure keys **as the set which includes the keys originating from** p **and** q **and expressed as (1), f_0 ***denotes threshold of security strength**, **and** f_{max} **denotes the maximum of security strength**, **function** keys(p, q, s_i) **return the number of keys deprived from prime pair*** (*p*, *q*) of ***which security strength equal to** s_i.*

$$s(p,q)=\sum_{s_i=f_0}^{f_{\max}} keys(p,q,s_i) \qquad (1)$$

3.3. Lemma 1

Given two strong prime pair (*p* , *q*), ***the security strength of its keys s is a factor of Euler function value of*** $\varphi[(p\text{-}1)(q\text{-}1)]$. For example, 8×280=2240； 1232×16=19712.

3.4. Lemma 2

***Given a security strength of some RSA key pair** f_1, **there always exists** f_2 **subjected to** $f_1 \times f_2 = f_{max}$.* For example, *p*=59,*q*=83, 1×280=2×140=70×4=56×5=40×7=35×8=28×10=20×14。

Due to space limitation, the mathematical proof about these two lemmas aren't provided here, details in the reference [5].According the description and examples above, the secure strength of key is a factor of its responding Euler value of (*p*-1) (*q*-1). The keys with different secure strength and it with different amount. But how to choose secure keys? It is essential to give the definition of threshold of secure strength.

3.5. Definition 3: threshold of Security Strength

Given two strong primes** p **and** q, **divide Euler function value of $\Phi[(p\text{-}1)(q\text{-}1)]$ ***by*** 2 ***recursively so as to get an odd number which denoted by** $f_0(p, q)$, **abbreviated by** f_0, **defined as the** threshold of secure strength **of the keys originated from the prime pair*** (*p*, *q*). For example $f_0(59,83)=35$； f_0 (179,227)=77.

Under the condition of having known the plain-text, the attacker would launch known plaintext attack against RSA. That is to attempt to search *a*. In order to defeat this motive, f_0 ought to be kept as bigger as possible. In the case of both *p* and *q* being strong primes,. the Euler function value of $\Phi[(p\text{-}1)(q\text{-}1)]$ *can* be calculated as (2).

$$\varphi((p-1)(q-1)) = 4p_1q_1\frac{p_1-1}{p_1}\frac{q_1-1}{q_1}\frac{1}{2} = 2(p_1-1)(q_1-1) \qquad (2)$$

Is it is possible to defeat this attack if properly to choose prime p_1 and q_1? The key of anti-attack avoids the existence of a far smaller number *s* referred above than f_0. However, in the precondition of p_1 and q_1 being strong primes, the existence of a small *s* hasn't being demonstrated yet mathematically. In the most construction of security system or security middle–ware, this issue is neglected in the module to implement RSA algorithm, which buries an indiscoverable bomb for the security of information [9,10].

4. Experimentation And Statistics Analysis

In the course of experiment, most operation of the testing security strength is modulus exponential, which requires a high cost of time and space. For the goal of bettering running speed, much implementation introduces some improving steps. For example, taking a share and fixed public key exponential u on encrypting, and while decrypting, saving the key parameters p and q, by Chinese Remainder Theorem reducing a big modulus into a small one, but not being computing the modulus exponential of a big integer, all of which speeds the crypto computations greatly.

Experimentation is operated on the computation platform of a high performance cluster, named Deep-Comp 1800, which computes the security strength of a 512-bits RSA keys. Data about it are as follows.

The private key strong prime p (Decimal digits：60, bits：197)：

179435497717087474860077696993008041829964087493290639987747.

The private key strong prime q (Decimal digits：95, bits：316)：

94126736627814276541856940222347804216056046459117311106921040158225173013787889116432788449223.

The public key modulus n (Decimal digits 155, bits：514):

33779355670594125240484931885103672392873747987436800715083532102739273112346435673197116904515578222884876485331404384775310539687299524405833722343328909.

$\Phi[(p\text{-}1)(q\text{-}1)]$ (Decimal digits：155, bits：513)：

16889677835297062620242465942551836196436873993718400357541483671159753113343592265777891408844871790056485259520091312721691082261863452404327626846335168.

The maximum odd factors of $\phi[(p\text{-}1)(q\text{-}1)]\,f_0$ (Decimal digits：153, bits：507):

263901216176516603441288530352372440569326156151850005586585682361871142395993629152779553263201121719632582180001426761276423160341616443817619169473987.

Aim at p ,q, the running time details shown as Table 1(no speeding) and table 2 (speeded by CRT).

However, it makes it a condition that the prime factors decomposition expression of $\phi(p\text{-}1)(q\text{-}1)$ is extracted. Obviously $GCD(2^k,f)$=1,let $m_1=2^k$,$m_2=f$; then $M= m_1 \times m_2$, let $M_1=M/\mathrm{m}_1$； $M_2=M/m_2$； extract y_i subjected to $y_i \times M_i \equiv 1 \bmod m_i$； compute $a_i= modexp(u,f,m_i)$； $x \equiv a_1M_1y_1+a_2M_2y_2 \ mod\ M$. According to CRT, $x = modexp(u, f,(p\text{-}1)(q\text{-}1))$,that is the result.

TABLE 1. REGULAR RUNNING TIME

Bits	Decrypt (ms)	Encrypt (ms)
256	16	1
512	16	2
1024	94	31

ms: Millisecond

TABLE 2. RUNNING TIME BY CRT ACCELERATION

Bits	Decrypt (ms)	Encrypt (ms)
256	9	1
512	10	2
1024	57	31

ms: Millisecond

We sample the data of a strong 512-bits RSA key pair which is listed as above. And its security coefficients f_0 is extracted at the cost 8810ms. If it is in use, it takes f_0 times encryption operation, about $10^{153}\text{ms}\approx10^{143}$ years on the computer which can execute once encryption operation per 15ms in order to attack it by repeat encryption. Through a process like that, the security strength quality of key is recognized quantitatively and clearly, and the probability of introduction of weak at random key is cut largely.

5. Conclusion

Customarily, people tend to relate the security of system to crypto algorithm, and most of focus on security is placed on algorithm. As a matter of fact, strength is a fundamental characteristic of key. As to strong algorithm there are chances of generating weak keys, which puts the information security in the danger of collapse. It is possible and necessary to quantitatively recognize the security characteristic of key and to treat it as one of the candidate criterions. In the paper a practical solution against the issue in the discussion is initiated, which can promote the recognition to RSA and improving its security. Several pieces of conclusion are summarized as follows.

1. Against the known plaintext attack to RSA public key crypto scheme, the concept of key security coefficient, the evaluation model of security coefficient and the algorithm to extract security coefficient are pioneered systematically in this paper. In addition, the security performance of key and the responding experimental statistics is extracted and analyzed thoroughly.

2. Via a process as this, key security quality is recognized quantitatively and clearly, and the probability of introducing weak key at random is cut largely. In a word, our mechanism could improve the security of RSA in effect which is demonstrated by the theoretic analysis and statistics above.

Acknowledgements

This work is Supported partially by the Provincial NSF Project of Hunan, China, with No. 09JJ6086.

Wenxue Tan (1973-). He is an Associate Professor engaging in teaching in College of Computer Science and Technology, Hunan University of Arts and Science. His current research interests include Artificial Intelligence, Network and Information Security.

Xiping Wang (1979-). She is a Lecturer engaging in scientific researching and teaching in Hunan University of Arts and Science. Her research interests include: AI and E-Commerce.

Xiaoping Lou (1982-). She is a Lecturer engaging in scientific researching and teaching in Hunan University of Arts and Science. Her research interests include: Applied Cryptography.

Meisen Pan (1971-). He is a Professor engaging in scientific researching and teaching in Hunan University of Arts and Science. His research interests include: Image processing.

References

[1] R. Steinfeld and Y. Zheng. An advantage of low-exponent RSA with modulus primes sharing least significant bits. Proceedings of RSA Conference 2001, Cryptographer's Track, Lecture Notes in Computer Science, vol. 2020,Springer-Verlag, pp. 52–62, 2001.

[2] HAN J, ZENG XY, TANG T A. Power trace analysis attack and counter measures for RSA cryptographic circuits. Chinese Journal of Computers, Vol.29,no.4,pp:590-595,2006.

[3].F.R Henriquez and C.K.Koc, Parallel Multi-Pliers Based on Special Irreducible Polynomials, IEEE Transactions on Computers,vol.52,no.12, pp.1535-1542, 2004.

[4] CHEN Huafeng, SHEN Haibin and YAN Xiao Lang, Characteristics of Parameterized Chaotic Map on Security and Implementation, Chinese Journal of Electronics,Vol.16,No.4 ,pp.627-630, 2007.

[5] Tan Wen-xue, Guo Guo-qiang, Research and analysis on model of testing and quantitating strength about RSA keys, Computer Engineering and Design,Vol.28 No.22,pp:5370-5374,2007.

[6] H.Fan and Y.Dai, Fast Bit-parallel GF(2^n) Multiplier for All Trinomials, IEEE Transactions on Computers,vol.54,no.4,2005,pp.485-490.

[7] Coron J S, May A. Deterministic polynomial time equivalence of computing the RSA secret key and factoring . Journal of Cryptology,Vol.20,pp:39-50,2007.

[8] S.J.Li, X.Zheng, X.Q.Mou, Chaotic encryption scheme for real-time digital video ,Proceedings of SPIE, Real-Time Imaging VI,pp.149-160. 2002.

[9] Zheng Yonghui, Zhu Yuefei, Xu Hong,A cycling like attack on RSA, Huazhong Univ. of Sci. & Tech. (Natural Science Edition),Vol.37 No.12,pp 56-60,2009.

[10] Wang G L, Feng B, Zhou J Y, Deng Robert H. Comments on A Practical(t,n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem. IEEE Transactions on Knowledge and Data Engineering, Vol.16,no.10,pp:1309-1311,2004.