Modern Management based on Big Data III
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220107

Review of Li-Li Mixture XOR Algorithm

Jie-feng YANG[1,a] , Li-shan HUANG[b] and Cheng-lian LIU [c]

[a] *Department of Science and Technology, Shiyuan College of Nanning Normal University, Nanning 530000, China*

[b] *School of Management, University of Pacific, Nicaragua*

[c] *School of Computer Science, University of Pacific, Nicaragua*

Abstract. RSA is one of the well-known public key cryptography algorithms (asymmetric encryption cryptosystem) , it has been more than 40 years since it was put forward. There are countless literatures on RSA related issues; hot discussion and popularization in academic and industrial circles, it is one of the typical public key cryptosystems. The reliability of RSA algorithm mainly depends on the factorization of large integers mentioned in the principle of RSA algorithm because it is extremely difficult to factorize very large integers. Unfortunately, there is no sufficient way to break the RSA. Due to the low efficiency and decryption speed of RSA computing, many scholars are committed to improving the efficiency of RSA algorithm, Ping Li and Yong Li's algorithm (hereinafter referred to as Li-Li algorithm) is one of the research literature. A hybrid encryption algorithm based on XOR operation proposed by Li-Li has defects, this defect is not easy to detect, this paper will point out the problem and give examples to prove the authors claims.

Keywords. RSA algorithm; XOR operation; Large number decomposition problem

1. Introduction

With the development of information technology, today's society has entered the information age, that is, based on modern communication network and database technology, collect relevant information into the database. However, in the process of information exchange and transmission, it also faces many security risks. Our personal information, computer hardware, software and data have been maliciously or accidentally damaged, tampered with and leaked. In August 2013, the data leakage of YAHOO [1] had caused the information of more than 1 billion users to be leaked; In March 2017, a major data leakage event occurred at AJL[2]. A hacker hacked 4 million 800 thousand related personnel 'data through loopholes, And so on. RSA was one of the

[1] Corresponding Author, Jie-feng YANG, Department of Science and Technology, Shiyuan College of Nanning Normal University, Nanning 530000, China, Email: 390037931@qq.com

This paper is partially supported by the university students' innovation and entrepreneurship of Guangxi Zhuang autonomous region under the project number 202213642016.

well-known non dual encrypted techniques. This makes us more aware of the importance of personal information protection. Therefore, in order to better and faster guarantee the transmission of information files, people have developed some better calculation methods for confidential information files. RSA was one of the well-known non dual encrypted techniques.

Table 1 — Related Literatures

Particular year	algorithm	autograph	Cloud app	other
2010		Fang et al.[3]		
2011		Liu and Zhan[4] Liu et al.[5]	Zhang et al. [17]	
2012	Guo and Liu[6]			
2013	Li and Li[7]			
2014	Liu et al. [8]			
2015				Liu et al. [9] Wu and Liu[10]
2016				Zhang et al. [11]
2017				Yan et al. [12]
2018	Ye et al. [13]			Zhang et al. [15]
	Fang and Liu[14]			Liu et al. [16]
2019	Liu and Xu[18]		Chen and Liu[19]	
2020	Yang et al. [20]		Zhong et al. [21]	

RSA had a wide range of applications, and its application in digital signatures was like that in documents [3, 4, 5], The discussions on cloud advertising and security were like [17, 19, 21], and the most extensive ones were about the research on the calculation itself, like [6, 7, 8, 13, 14, 18,20]. RSA can also be discussed in conjunction with other fields, such as the contact with Goldbach [9], the application of anonymous express information system [10], the application of internal control of enterprises [11,12], the application of free card bank mobile payment [15], the application of [16] for anonymous complaints, and so on. All show that people are deeply interested in RSA. See Table 1 for details.

2. Review of Li-Li algorithm

The ideas of Li Ping and Li Yong (hereinafter referred to as Li-Li algorithm) [7] are mainly through XOR operation and RSA algorithm [22]. The encryption of key and plaintext makes the speed of information encryption faster, so a hybrid encryption algorithm based on XOR is proposed. In this section, we will introduce the principle of RSA algorithm in sequence, and then introduce the operation idea of Li-Li algorithm, as shown below.

2.1 The of RSA algorithm

RSA is a public key cryptography algorithm. Its name is composed of the initials of the last names of several developers, namely Ron Rivest, Adi Shamir and Leonard Adleman. RSA algorithm uses different encryption keys and decryption keys to encrypt information, which ensures that the information will not be decrypted and disclosed by

others in the process of transmission. However, the efficiency is low and the process of encryption and decryption is slow. Principle of RSA algorithm: According to the elementary number theory, the number obtained by multiplying two prime numbers is used as the public key, it is extremely difficult to decompose this product into the original two prime numbers, that is, the so-called large number decomposition problem. There are many literatures on large number decomposition, but there is no effective method to decompose large numbers. RSA shows its security based on the premise of the difficulty of large number decomposition.

The principle of RSA algorithm is as follows:

step 1. Randomly select two prime numbers p and q ,and calculate

$$n = p * q \quad (1)$$

step 2. Then calculate

$$\varphi(n) \equiv (p-1)(q-1) \quad (2)$$

step 3. Randomly select a public key value e , to satisfy $\gcd(e, \varphi(n)) = 1$, and calculate the value of as follows

$$e * d \equiv (mod\ \varphi(n)) \quad (3)$$

step 4. A message m is encrypted to obtain ciphertext C , which is calculated as follows

$$C \equiv m^e (mod\ n) \quad (4)$$

step 5. The more the ciphertext C is restored, the following operations are performed

$$m \equiv C^d\ (mod\ n) \quad (5)$$

The order of the above equations from (1) to (5) is the famous RSA algorithm principle. The public key pair parameter is $\{n, e\}$, and the key pair parameter is $\{n, d\}$, according to the principle of RSA algorithm, parameter $\{p, q, \varphi(n), d\}$ is not public, and only n and e are public.

2.2 The Li-Li Algorithm

Based on Li Ping-Li Yong algorithm, it is assumed that Alice, the publisher, encrypts and transmits C_p and C_k to Bob, the receiver, and Bob uses the key given by Alice combined with XOR operation to decrypt and restore C_p and C_k . The specific Li-Li algorithm is shown in Figure 1.

step 1. Alice randomly selects a k value and performs XOR operation on message m and k , as shown in equation (6).

$$C_p = m \oplus k \quad (6)$$

step 2. Use RSA public key e to encrypt its k , see equation (7).

$$C_k = k^e (mod\ n) \quad (7)$$

Then transfer and to Bob.

step 3. When Bob receives C_p and C_k from Alice, he first uses RSA key d to obtain the value of as follows

$$k \equiv (C_k)^d (mod\ n) \quad (8)$$

step 4. After obtaining k , k is used to XOR C_p to restore the content of message m .

$$m = k \oplus C_p \quad (9)$$

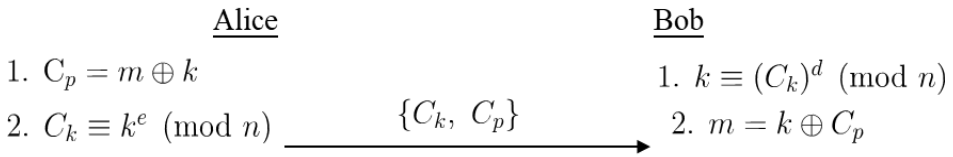

Figure 1. Li-Li algorithm protocol diagram

Equations (6) to (9) are the essence of the Li-Li algorithm.

The beauty of the Li-Li algorithm lies in:

1) In the process of communication between the two sides, the message m is not transmitted. The attacker cannot calculate the message m through the intercepted C_p and C_k . based on this, Alice and Bob do not have to worry about disclosing the content.

2) During transmission, the key values k and d are not present, and it is impossible for an attacker to obtain this value from empty space.

2.3 Data from experimental results

1) Randomly select two prime numbers $p = 27$ and $q = 73$, and calculate $n = 27 * 73 = 1917$.

2) Suppose $e = 29$, and $\varphi(n) = 1872$, because $\gcd(e, \varphi(n)) = 1$, then $d = 581$.

3) Assume that the message is digitized to $m = 70$.

4) Randomly select k value as $k = 79$.

5) Calculate $C_p = 70 \oplus 79 = 9$.

6) Calculate $C_k \equiv 79^{29} \equiv 1921\ (mod\ 1971)$ and pass C_p and C_k to Bob.

7) Bob calculates the value of k after receiving C_p and C_k .

$k \equiv 1921^{581} \equiv 79\ (mod\ 1971)$.

8) Calculate the m value again,

$m = 79 \oplus 9 = 70$.

The above is the calculation process and experimental data of Li-Li algorithm.

3. Our comments

Li Ping-Li Yong algorithm proposed a new hybrid encryption algorithm. The security of this algorithm is the same as that of RSA algorithm. When the algorithm communicates with each other and does not transmit information m , the second cannot read m . For RSA algorithm, the initial version uses the Euler function [23] $\varphi(n)$. However, in order to improve computational efficiency while maintaining the same security, in the second version of the RSA algorithm modification [24], has been changed to $\lambda(n)$, as follows

$$\lambda(n) = (p-1, q-1) = (26,72) = 936 \qquad (10)$$

Is there a number y and it is satisfied

$$m^{\varphi(n)} \equiv m^{\lambda(n)} \equiv m^y \equiv 1\ (mod\ n) \qquad (11)$$

It is known from reference [8] that whether there is a more efficient method to solve $y = 36$ as one of the methods to calculate y is our follow-up work.

4. Conclusions

To sum up, whether there is a y for n generated by any prime numbers p and q to meet equation (11) is a problem worthy of discussion, which is not only related to the security of RSA algorithm, but also discussed by number theory or computer algorithm. For solving y, it will be listed as the research direction in the future.

References

[1] Xinhua news agency, the data leakage incident that happened in YAHOO in August 2013, caused more than 1 billion users' information to be leaked, Xinhuanet, http://www.xinhuanet.com/world/2016-12/16/c_129406345.htm, 2016-12-16.
[2] C114 China communications network, shocking 2017 inventory of ten major data leakage incidents, thousands of WeChat official account, http://www.qianjia.com/html/2018-01/12_282375.html, 2018-01-12.
[3] Dejian Fang, Na Wang, Chenglian Liu. An Enhanced RSA-based Partially Blind Signature, International Conference on Computer and Communication Technologies in Agriculture Engineering (CCTAE 2010), June 12-13, 2010, Chengdu, China, pp. 565- 567.
[4] Chenglian Liu, Jinsong Zhan. Comment on an Enhanced RSA-Based Partially Blind Signature, Applied Mechanics and Materials, Vol. 71-78, pp. 3207-3212, 2011.
[5] Chenglian Liu, Marjan Kuchaki Rafsanjani, Liyun Zheng. Comment on the Improvement of an Efficient ID-based RSA Multisignature, Second International Workshop on Trust Management in P2P Systems, Kochi, Kerala, India, July 22-24, 2011.
[6] Yongning Guo and Chenglian Liu. Comment on a Research and Analysis Four-Prime RSA, Advances in Electronic Engineering, Communication and Management, Vol. 2, Volume 140 of the series Lecture Notes in Electrical Engineering, pp. 669-675, 2012.
[7] Ping Li and Yong Li. A mixture encryption algorithm based on XOR operation, Journal of Qujing Normal University, Vol. 32, No. 3, pp. 39-42, May 2013. (Chinese version)
[8] Chenglian Liu, Yongning Guo and Juan Lin. Security analysis of RSA cryptosystem algorithm and it's properties, AIP Conference Proceeding, Vol. 1618, pp. 468-470, 2014.
[9] Chenglian Liu, Chin-Chen Chang, Zhi-Pan Wu and Shi-Lin Ye. A Study of Relationship between RSA Public Key Cryptosystem and Goldbach's Conjecture Properties, International Journal of Network Security, Vol. 17, no. 4, pp. 445-453, 2015.
[10] Jieling Wu and Chenglian Liu. A Study of Anonymous Delivery Based on Blind Signature Scheme, Procedia Computer Science, Vol. 52, pp. 1065-1070. 2015.
[11] Xiao-Tong Zhang, Chenglian Liu and Jie Fang. Study of Enterprise Internal Control Based on Dual Complexity and Anonymity Information System, Journal of Fuqing Branch of Fujian Normal University, Vol. 5, No. 138, pp. 27-34, 2016.
[12] and Donald Gardner. Weakness of RSA cryptosystem characteristic, International Conference of Computational Methods in Sciences and Engineering 2018 (ICCMSE 2018), AIP Conference Proceedings, Vol. 2040, pp. 130005-1–130005-7, 2018.
[13] Han-Bing Yan, Chenglian Liu and Lin-Shan Huang. Comment on Zhang et al.'s Anonymous Information Scheme, Journal of Fuqing Branch of Fujian Normal University, Vol. 2, No. 141, pp. 23-29, 2017.
[14] Jie Fang and Chenglian Liu. A Generalize Estimating the of Upper/Lower Bound to RSA Public Key Cryptosystem, International Journal of Network Security, Vol. 20, No. 2, pp .332-336, March 2018.
[15] Cheng Zhang, Yong-Zhang Luo and Chenglian Liu. A Dynamic Passcode System for Mobile Purchasing Without Bank Card, The 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP' 18), December 26-28, 2018, Taipei, Taiwan.
[16] Chenglian Liu, Chien-Wen Hsu, Chunyuan Tao and Guangpu Chen. Study of anonymous based on the Letters and Visits Information System, Journal of Fuqing Branch of Fujian Normal University, Vol. 2, pp. 46-52, 2018.
[17] Jian Hong Zhang, Xue Liu, Cheng Lian Liu. A RSA-Based Data Integrity Check without Original Data in the Cloud Computing, Applied Mechanics and Materials (AMM), Vol. 44-47, pp. 3726-3730, 2011.
[18] Chenglian Liu and Chieh-Wen Hsu. Comment on "Improved Secure RSA Cryptosystem (ISRSAC) for Data Confidentiality in Cloud", International Journal of Network Security, Vol. 21, No. 4, pp. 410-413, 2019.

[19] Sonia C-I Chen and Chenglian Liu. Comment on Secure File Storage and Retrieval in Cloud, 17th International Conference of Numerical Analysis and Applied Mathematics, September 23-28, 2019, Greece.
[20] Guiyu Yang, Hongxuan Liu, Chenglian Liu and Sonia C-I Chen. Comment on MRSAC Scheme, The 9th International Conference on Industrial Technology and Management (ICITM 2020), 11-13 February, 2020, St Anne's College, University of Oxford, UK.
[21] Zhengrun Zhong, Hongxuan Liu, Sonia C-I Chen, Chenglian Liu and Donald Gardner. Comment of Secure File Storage and Retrieval in Cloud Based on MRSA Cryptographic Algorithm, The 9th International Conference on Industrial Technology and Management (ICITM 2020), 11-13 February, 2020, St Anne's College, University of Oxford, UK.
[22] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.
[23] Euler totient function Wikipedia website, 2019-02-02.
[24] Carmichael totient function Wikipedia website, https://en.wikipedia.org/wiki/Carmichael_function, 2019-02-02.