SURVEY ON ASYMMETRIC ALGORITHM USING RSA DIFFERENT MODIFIED MODELS

San San Tint

University of Computer Studies, Mandalay, Myanmar

ABSTRACT

In the Internet we have been searching different kinds of papers describing Cryptography technique imposed by many algorithms. Almost papers published in the Web are used popular algorithms. Among them RSA is a very popular algorithm for security in the Web. We use attributes to summarize in the RSA algorithm by means of well known parameters. Some papers are thought about cloud and others for different environments. There is motivated to collect and summarize what are differences between them. This paper focuses on a comprehensive analysis of different modified RSA algorithms and supplies the recognition of RSA intensively. Most of sections are well composed for detail explanations about papers studied as a list of numbers and a table.

KEYWORDS

Cryptography, RSA, Popular Algorithm, Parameters, Differences

1. INTRODUCTION

In the world the technologies are improving day by day without knowing anybody. In fact, humans living in the world wants more convenient and more security even though they have facilities more than their needs. At present security is able to be more possible for lives to be taken long living without worries. Some researchers tried to summarize to be obvious the differences among existing algorithms how to be more reliable and what are needed to improved to be more useful one [1-4].

Cryptography involving algorithms for applications is the most technique in security. The growth of information is essential part of real world because of wide areas of technology and applications. As a result, products of cryptography are demanded as innovations. Roughly, Cryptography can be divided into two things such as Symmetric key algorithm and Asymmetric key algorithm. Symmetric key algorithms are also known as secret key, single key, one key and private key. Asymmetric key algorithms are called public key algorithm in which encryption and decryption are mathematically performed using different keys. We define one key is a public key and another is a private key. Some popular and well known asymmetric algorithms contains Diffie-Hellman keys, SSH, SSL, DH and RSA [2].

Most kind of cryptographic techniques are intended to be secure and the researchers want to find out a matter as an answer without severe complexity. By collecting the modified RSA algorithms, people who those are supporting for secure transmission in network are assisted something for thinking about reliable portion in communities [2, 3].

2. RSA CRYPTOGRAPHY TECHNOLOGY

2.1. Asymmetric Key Algorithms

Asymmetric encryption is a one of the different forms of cryptosystem. It has two parts known as encryption and decryption performed using the different keys—one a public key and one a private key. It is also known as public-key encryption. As we know, we can use Asymmetric encryption to transforms plaintext into ciphertext. There is a key pair to use transferring time for data security. To protect from some hackers, most of people want to choose more reliable system like RSA. Among famous cryptography techniques, RSA is the most useful one to protect from attack because of the difficulty of finding the prime factors of a composite number [5].

2.2. Public-Key in Cryptosystems

The concept of public-key cryptography derived from an attempt to intercept message between persons who have symmetric encryption. Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic. It is very difficult to guess a key computationally although they have the decryption key given only knowledge of the cryptographic algorithm and the encryption key [5, 6].

2.3. Public and Private Keys of Cryptosystems

There is a selected key pair in which one for encryption and other for decryption in one side. So we can use random prime numbers at a time for one side. According to the public or private key, the exact transformations will be performed by the algorithm as well as inputs [6]. The security of transmission depends on two keys in which both a sender and a receiver know their keys in RSA algorithm. In RSA key, there are three categories as follows:

1. Short key's range is less than the 900 bits,
2. Medium key's range is between the 900 and a250 bits and
3. Long key's range is greater than 1250 bits.

2.4. Description of the RSA Algorithm

Between a sender and a receiver, following steps are needed to get successful transmission.

1. RSA uses an expression with exponentials.
2. Every block equal to a binary value less than some number n.
3. The block size must be less than or equal to $\log_2(n) + 1$; where $2^i < n \leq 2^{i+1}$.
4. Both sides must know the value of n.
5. Encrypt for some plaintext block M and decrypt for ciphertext block C.

6. The side knows the value of e, and only the another side knows the value of d.
7. A public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d, n} on one side.
8. In this algorithm for public-key encryption,

- It is possible to know values of e, d, n such that M^{ed} mod n = M for all M < n.
- It is not difficult to calculate M^e mod n and C^d mod n for all values of M < n.
- It is difficult to determine d given e and n.

The above relationship means if e and d are multiplicative inverses modulo φ(n), where φ(n) is the Euler totient function.

- p, q primes, φ (pq) = (p - 1)(q - 1).
- Relationship between e and d as ed mod φ(n) = 1.
- Both e and d are multiplicative inverses mod f(n).

By the rules of modular arithmetic, only if d is relatively prime to f(n). Equivalently, gcd(f(n), d) = 1.

RSA scheme has following:

- p, q, random prime numbers
- n = pq
- e, with gcd(f(n), e) = 1; 1 < e < f(n)
- d K e-1 (mod f(n)) The private key consists of {d, n} and the public key consists of {e, n}.

Assume that user A has published his or her public key and that user B wishes to send the message M to A.

Then user B calculates $C = M^e$ mod n and transmits C. When user A gets this ciphertext, user A decrypts by calculating $M = C^d$ mod n[5,6].

Figure 1 shows the continuous sequential steps for traditional RSA algorithm.

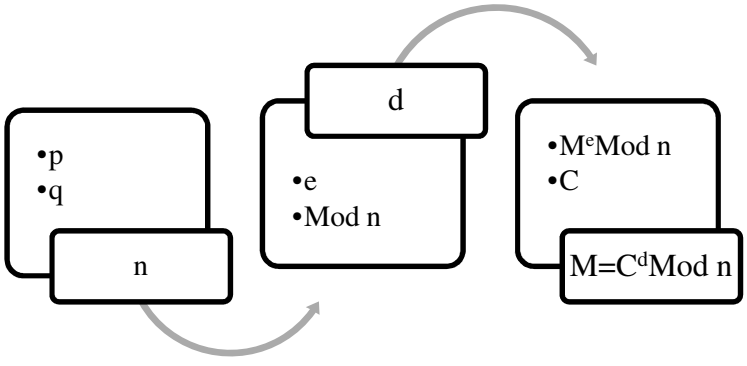

Figure 1. Sequential Steps of RSA

3. SCOPE OF THIS PAPER

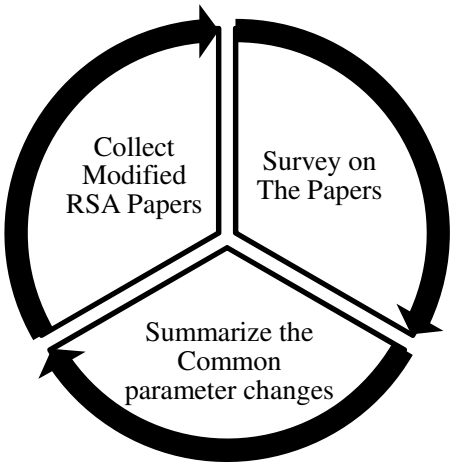

Figure 2. Paper Scope

Above figure 2 shows how to consider this survey paper and this figure means that it needs to carry on in future like this paper continuously.

4. SURVEY ON PAPERS RELATED RSA FOR DIFFERENT MODELS

The paper [1] made me motivated to survey on different types of modified RSA papers as well as all parameters that are important for security in every environment. Although RSA is highly secure algorithm, environments demand to modify according the challenges of security in the world day by day. It described many researchers increase the speed of traditional RSA algorithm by various techniques.

1. The reference paper mentioned different 'e' value for specific message block size in network. The sender will be allowed a message by algorithm to generate a public key to encrypt the message and a generated key will be sent to receiver.
   By using incorrect private key in RSA algorithm, the encrypted message will not be form to original message. In that paper, 'e' value is changed to be another one what minus '1' in to $\Phi(n)$ so that the modified one is more secure than existing algorithm[7].
2. In [8], it covered secured storage and applies method for cloud environment and also supported the modern Cryptography concept for data security in cloud. It can be seen to be concern enterprises and vendors to access centralized shared hardware, software and other information.
   It obviously explained that the strength of cloud computing is essential ability for mass resources. Two distinct bits and small humming weight are used in RSA modified model.
3. The modified RSA algorithm presented BIT STUFFING RSA idea by using 512 bits to be more secure. They used bit stuffing for various purposes like bring bit streams. The stuffing bits location is connected with the receiver.
   To synchronize several channels bit stuffing is used for communication time. Before sending the receiver, the stuffing bits are added into the encrypted message as random

number. In receiver side, after receiving, he or she must extract the stuffing bits from ciphertext [9].

4. They implemented Double RSA with the cooperation of the sender and the receiver of the data. Double RSA has four keys that e and g are public keys and d and h are private keys. The procedure has been assumed that (e, d) pairs of keys and modulus N belongs to the receiver and (g, h) pairs of keys and modulus N1 belong to sender.
   Double modulo RSA for keep information confidential in the unsecure network is implemented $C(s)=M^e$ Mod n and $C(r)=M^e$ Mod n_1 at first and second stage of transmission and gathered the public and private key pairs which were applied in the 3rd stage where the original message was to be received by the receiver [10].
5. Authors proposed RSA-based password-authenticated key exchange (RSA-PAKE) protocols for imbalanced wireless networks where a party uses a low-power device to communicate with another party equipped with a powerful computing device.
   Today, there is the most important to reduce the cost of communication for a low-power device even though the cost for powerful devices is increasing. The reliability of unauthorized RSA public keys is be able to design an efficient reliability test method to construct an efficient RSA-PAKE protocol like the most power-consuming operation. It used especially for probability bit [11].
6. In [12], the paper used two key pair in which one small size key pair for data encryption and one large size key for encrypt key. The weakness of existing RSA cryptosystem is the component n=p*q of small size key pair since both small n and large n lead to more time consuming in encryption and decryption.
   The proposed system is compared the efficiency of existing RSA since it takes less time than existing one.
7. It consists of k primes ($N = p_1*p_2*\ldots*p_k$) for the software implementations of RSA algorithm based on 2-prime RSA. Modified the RSA has multiple primes not including the traditional two primes p and q.
   The RSA implementations with the multi-prime RSA speed up to decrypt the data four times faster than the classic RSA. There are four prime numbers in algorithm such as p, q, r and s where $p \neq q \neq r \neq s$ and both p, q, r, s are prime numbers and also determine n = p x q x r x s [13].
8. The number of primes used in the paper is only difference between RSA and Multi-prime RSA algorithm. They give assumptions about Multi-prime RSA with r- primes, r >2. The modulus, $N = \pi^r_{i=1} p_i$ for r distinct primes.
   So they need to calculate $M_i' = C_i^d \bmod p_i$ for i times, i >2 and randomly chosen distinct primes $p_1,\ldots, p_r$. The secret exponent d is larger than the public exponent e. They said that the Multi prime RSA is less vulnerable to attacks on RSA because of increasing the number of prime factors in the modulus [14].

All of papers for my survey have some constructive capacities with famous purposes like as follow:

1. Non Complex architecture,
2. Scalability,
3. Flexibility,
4. Reliability,
5. Security.

5. SUMMARY OF SURVEY PARAMETERS

Table1. Summary of Characteristics of Parameters

Ref: no	p & q	e	d	n	M	C
7	Prime	(p-1)(q-1)	e^{-1}(Φ(n)-1)	p*q	C^d Mod n	M^e Mod n
8	Two distinct prime no:	Short bit	e^{-1}(mod Φ(n))	p*q	C^d Mod n	M^e Mod n
9	Two large prime	choose from e*d=1.mod (p-1)(q-1)	e^{-1}(mod Φ(n))	p*q	C^d Mod n	M^e Mod n + some word
10	prime	Two public key e ,g	Two private key d ,h	p*q	C^d Mod n	C(s)=M^e Modn C(r)=M^e Modn_1
11	distinct primes	ℓ*e*-bit prime or chosen ℓ*e*-bit pseudo prime	e^{-1}(mod Φ(n))	p*q	C^d Mod n	M^e Mod n
12	Small size key pair & large size key pair	1<e<f(n)	e^{-1}(mod Φ(n))	p*q	C^d Mod n	M^e Mod n
13	Four prime numbers(p,q,r,s)	e_1,e_2,e_3,e_4	e^{-1}(mod Φ(n))	*p* x *q* x r x s	C^d Mod n	M^e Mod n
14	Randomly chosen distinct primes p_1,...,p_r	N^{α}	d_i ´=dmod (p_i - 1)	$N = \pi^r_{i=1} p_i$	M_i´=C^d_i mod p_i	M^e Mod N

On the papers concerned with modified RSA algorithms, researchers assumes to create to develop able to be speed up and more secure in their proposed systems. Typically, some parameters are well known for readers interested in cryptography technology technique. Especially, they introduced and eager to change the well known parameters such as p, q, e and d in Table 1. They denoted the difficulties to find the original message from encryption message because of their achievement while eavesdroppers were trying to intercept their own message. But their outcomes contained some unacceptable results what no one knows how to solve the problems like complexity, time consuming, waste memory and so on.

They thought about their modification on RSA algorithm strongly defended from intruders. Obviously, they can change value familiar parameters and calculate to somewhat reliable parameters. Another paper was demonstrated for n value from multiplication of random prime numbers [10].

6. AUTHORS PERSPECTIVE ON PAPERS

From the perspective of authors, there are needed to create RSA to be more secure. But there are different ideas between them. In some papers, authors assumed that random prime numbers are always applied and no need to modify [7-14]. They have similar idea on p and q [7-14]. Without altering asymmetric key, mostly they want to find new key or new value for public relation key e [13,14].

Others are hardly changed for public key e and private relation key d [7-12]. Only two of these papers are calculated with not only relative public keys but also four prime numbers because of the name of papers, multiple public key and multiprime [13, 14]. Usually they choose their plaintext, M that equals C^d Mod n. Although researchers have been seem rarely to modify the original message, modification the value M, e, d and n are change to modification ones in the last paper [14].

Even though they hardly find to how to crate to meet the original characteristics of RSA algorithm without wasting its abilities, researchers can do the experiments for several environments such as Network, Cloud, Secure socket layer and RSA-PAKE protocol [7-9,11]. This paper can express types of environment and number of bit stream in figure 2 according to their experimental results.

Table 2. Environment and Bit Nature

Ref: no	Environment	Bit
7	Network	p&q<=4
8	Cloud	Small humming weight
9	Secure socket layer	Stuffing some word
10	Brute force attack	Two -key pairs, n & n_1
11	RSA-PAKE protocol	Probability bit
12	-	Two different sizes
13	-	Multiple public keys
14	Multi prime	secret exponent d larger than the public exponent e

Among the papers I have read, those what take into account essential functions, authentication, integrity, non-reputation and confidentiality.

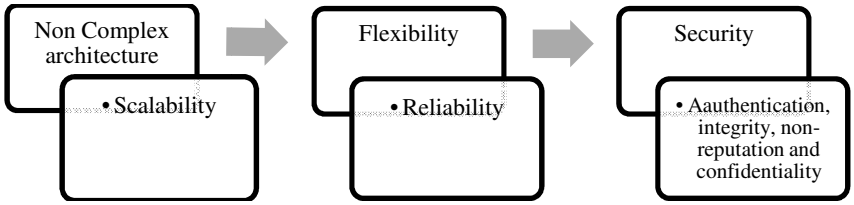

Figure 3. Essential Qualification for RSA

The goal of this survey paper is to observe how to modify the several modified RSA and what are differences between them. After observing, people who need to study about asymmetric key can apply to search another innovation that will be applicable for the communication in social world. Figure 4 prescribes to aim to be more applicable RSA.

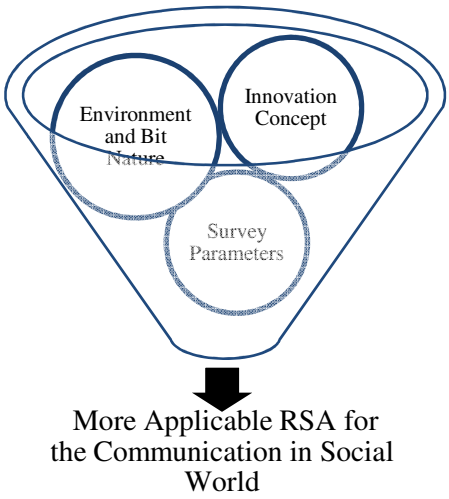

Figure 4. Model for Next RSA

7. CONCLUSION AND FUTURE RESEARCH ISSUES

In this paper, asymmetric key algorithm, RSA is evaluated by parameters in which modified RSA algorithms models. Almost models have some modifications that to be faster speed and more secure than existing RSA algorithm. We study various techniques such as original prime in network, two distinct prime and small humming, stuffing bits in cipertext on secure socket layer, two -different keys pairs in brute force attack, probability bit in RSA- PAKE protocol, two different size keys, multiple public keys and multi prime.

They mentioned that all modified RSA models they described met to get the achievements of needs in term of speed and security. This paper provides the knowledge which some of modified RSA algorithms are implemented to improve to be more secure although others are able to be speed up. Nevertheless, the complicated models are driven day by day and year by year. But they believe that whatever they do will be more useful than existing one.

As a future work, I will try to survey on other asymmetric keys and also about symmetric key in terms of security parameters counting Confidentiality, Authentication, accountability, and accuracy.

ACKNOWLEDGMENT

This paper is dedicated to our parents and my younger sister. The author would like to thank anonymous reviewers. And author thanks people who give their valuable explanation and suggestions on the paper. Our acknowledgments especially go to our families for their financial and moral support to the publication of this paper. Author actually thanks to people who motivate me to survey and to summarize for RSA algorithm from several papers in which Cryptography and Network Security related contributions are available. And author gratefully thank to people who wrote the papers I had read for this paper.

REFERENCES

[1] R. Tripathi and S. Agrawal, "Critical Analysis of RSA public Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering ISSN:2277-128x Volume4, Issue 7, July, 2014.

[2] M. Ebrahim, S. Khan, U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis".

[3] CS 6/7 75995 Advanced Internet- based Applications & Systems Design, "SURVEY PAPER", spring 2006.

[4] Anonymous Author, "Some thoughts about writing a survey paper", February 25, 2008.

[5] William Stallings," Cryptography and Network Security Principles and Practice", ISBN 13: 978-0-13-609704-4 Pearson Education, Fifth Edition.

[6] Behrouz. A. Forouzan, "Cryptography and Network Security", McGraw-HILL International Edition, 2008.

[7] N. Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", International Journal of Computer Science and Network Security, VOL.14, No.5, May, 2014.

[8] V. R. Augustine and Prof. P. L. Ramteke, "Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques", International Journal of Application in Engineering & Management, Volume 3, Issue3, March, 2014.

[9] Parshotam, R. Cheema and A. Gulati, "Improving the Secure Socket Layer by Modifying the RSA algorithm", International Journal of Computer Science, Engineering and Applications(IJCSEA), Vol.2, No.3, June, 2012. A.

[10] Gupta and V. Sharma, "Modified Double Mod RSA Tested with Brute Force Attack", International Journal of Innovative Research & Development, Vol. 3 Issue 5, May, 2014.

[11] J. Abudin, S. K. Keot, G. Malakar, N. M. Borah and M. Rahman, "Modified RSA Public Key Cryptosystem Using Two Key Pairs", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, p.3548-3550.

[12] T. Y. Youn, S. Lee, S. H. Hong and Y. H. Park, "Practical RSA-PAKE for Low-Power Device in Imbalanced Wireless Networks", International Journal of Distributed Sensor Networks, Volume 2014, Article ID 125309, May 2014.

[13] M. Sreedevi and M. Padmavathamma, "Multipair Public Key Cryptosystem", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 3 - May 2014.

[14] N. Ojha and S. Padhye," Cryptanalysis of Multi Prime RSA with Secret Key Greater than Public Key", International Journal of Network Security, Vol.16, No.1, PP.53-57, Jan, 2014.

Authors

Author is Associate Professor, Head of Department of Research and Development II in University of Computer Studies, Mandalay, Myanmar. Author has worked in University since 1997. Prior to that author spent 6 years as a teacher in Base Education School. Author got B.Sc.(Physics) and M.Sc.(Physics) degrees from Yangon University, Yangon, Myanmar in 1987 and 1996 and then M.A.Sc.(Computer Engineering) and Ph.D. (Information Technology) degrees from University of Computer Studies, Yangon, Myanmar in 2000 and 2004. Research and teaching in Cryptography and Network Security, Internetworking with TCP/IP and Digital Fundamental in University.