Enhancement of RSA Scheme using Agreement Secure Information for Nearest Parameters

Motasem A. Abu-Dawas
Computer Science Department
Irbid National University
Irbid, Jordan
Email: motasem_dawas [AT] inu.edu.jo

Abdulameer K. Hussain
Department of Computer - Faculty of IT
Jerash University
Jeresh, Jordan

Abstract—**This paper presents an effective solution to enhance the security of RSA scheme. The objective of this proposed method is to eliminate the redundant messages occurred in some values of n, the product of two prime numbers, and this is considered as a weak point in the RSA method. The solution depends on appending extra agreement secure information. This procedure enhances the security of RSA scheme because in case an attacker get the message is sent, he/she will face a difficulty to discover the original ciphertext.**

Keywords—cryptography; RSA; agreement; security; public keys

I. INTRODUCTION

In the current time, security is an important aspect to deal with because the existence of Internet which provides various ways of communication between multiple users. Cryptography is considered the most important effective way for the communication to be secure [1].

In the recent days, cryptography is extremely more complex than past .When we talk about modern cryptography, it generally refers to cryptosystems because it includes the study and practice of hiding information with the utilization of keys aspects. These are related with web based applications, ATM's, ecommerce, computer password, etc.

Generally, Cryptography is divided into two types of schemes: single key (symmetric/secret) key cryptography and multiple (asymmetric) key cryptography. A plaintext is the data which is to be encrypted in another form. Then this plaintext is encrypted into cipher text. Also this ciphetext must be decrypted again to recover the plaintext. One of the most important types of cryptography in the past is public key cryptography. Public key scheme involves two communicated parties in a secure communication without sharing their secret key over a non-secure channel, e.g. RSA [2].

RSA was introduced Ron Rivest, Adi Shamir and Leonard Adleman publicly in 1977 at MIT. It is considered one of the great achievements in the field of cryptography. RSA uses a public key to encrypt messages, and a private key to decrypt them. Security [3] is the core of this algorithm, for which, if the keys are properly chosen, it's not possible, or so computationally hard to become impractical, to decrypt the data unless you have the private key.

The strength of RSA depends on the fact that it is easy to multiply two large prime [4] numbers together, but extremely hard (i.e. time consuming) to factor them back from the result. Factoring a number means finding its prime factors (prime numbers) that need to be multiplied together in order to produce that number.

In RSA algorithm, the public is represented as a pair of integer numbers: e and n. The private key is a pair of integer numbers: d and n. The value of n is computed as the product of two prime numbers, p & q.

'd' is another prime number, bigger than p and q and 'relatively prime to p and q', for which exists an integer 'e', with this property:

$e * d = 1 \pmod{\varphi}$

Where $\varphi = (p - 1) * (q - 1)$

that is, the product of d and e, mod φ, e equals to 1, and said in other terms, 'd is the multiplicative inverse of e, modulus φ.

RSA algorithm is considered to be much slower when it is compared with DES and other symmetric cryptosystems. To overcome this problem, there is a lot of research work done in order to increase the speed of RSA algorithm. One of these researches is called Multi Prime RSA algorithm to improve the encryption speed of RSA algorithm.

This technique [5] was introduced by Collins who modified the RSA algorithm so that it consists of k primes p1, p2... pk instead of the traditional two prime's p and q.

Multi Power RSA gave the faster decryption/signature generation performance as compared to Multi Prime RSA [6].

The most effective way to protect information is cryptography which is an art of writing and reading the secret information. Cryptography is considered a method of encrypting the original information (message) into a form that is not interpreted by anyone. It is possible to recover the original message by decrypting the encrypted message. For such purpose cryptography uses public and private keys. Cryptographic systems can be categorized into symmetric and asymmetric systems. In symmetric cryptography, same key is used for the encryption and decryption whereas in asymmetric cryptography separate keys are used for the encryption and decryption process [7].

One way to enhance RSA algorithm is using three prime numbers to generate both the public and private keys. This enhanced RSA algorithm can enable faster encryption and decryption process and generates the public and the private key faster than the original RSA [8].

II. Related Works

In reference [9] a research for increasing the security of RSA algorithm by using two additional random values for the computation of N and hence to retain the similar decryption speed the value of N produced by only two prime number is used. That helps to retain the same decryption speed. Proposed algorithm will increase the factoring complexity of the standard algorithm up to minimum 6 times.

A paper introduced security enhancement on the RSA cryptosystem. This research suggests the use of randomized parameters in the encryption process to make RSA many attacks .This enhancement will make the RSA semantically secure, this means that that an attacker cannot distinguish two encryptions from each other even if the attacker knows (or has chosen) the corresponding plaintexts. A comparison introduced in this paper between the basic RSA and the modified RSA version shows that the enhancement can easily be implemented [10].

In addition we list below a group of related works found in [11].

Sun, Wu, Ting, and Hinek proposed new method of an RSA In this paper, the key generation algorithms output is two distinct RSA key pairs so both the public key and private key exponents are same. This variant method is within a family of alternative methods called dual RSA. This type of encryption has the advantage of reducing the data storage requirements of the keys [12].

In reference [13] the authors constructed a type of algorithm called k-RSA algorithm. In this type the idea of RSA algorithm and kth power residue theory is combined. In addition to the advantage of original RSA algorithm which depends on the factoring of large numbers and finding of discrete logarithms, this new construction adds a high flexibility of the parameters. This approach improved security and also achieve a balance between speed and space.

A new approach had been introduced which leads to harder encryption and also the enhancement of public key encryption protocol for security. This approach is helpful for sending secure email or any kind of message on internet [14].

III. Proposed Method

When RSA is implemented, there is a situation in which the ciphertext is the same as the plaintext in some values of n. So it is very important to find a solution for such a problem.

An effective solution to this problem is by changing the value cihertext by salting it with a secure agreement piece of information. If c is the ciphertext then we can append a secure piece of information s to both. In this case the ciphertext in the form of (c,s). For more security it is necessary to choose an alternative public key e' from a set of valid public keys and then generate the corresponding private key d'. The proper and secure method of selecting an alternative public key is by the agreement among parties upon the selection method. This is done by gathering all valid public keys in the range (0,..n-1) into subgroups and then choosing a secure and agreed distance r. The original public key is positioned at also a secure location in the set of all subgroups. We can then select an alternative public key depending on the value of both location of the original key and the distance of this location from one of the subgroups of public keys. In such a way, instead of encrypt the message m with the original public key e, the message will be encrypted with the alternative public key e'.

Upon receiving the ciphetext by the receiver, he/she removes the agreement information from the ciphetetext to get the original ciphertext. When the receiver extracts the agreement information then he can easily decrypt the ciphertext and recover the plaintext.

Algorithm:

```
Let R be the set of all subsets of public keys such that:
$R=\{\{e_1,\ldots.e_{n1}\},\{e_1,\ldots.e_{n2}\}\ldots\ldots\{e_1,\ldots.e_{nm}\}\}$
Let p and q be two large prime numbers
Let s be the agreement piece of information

Sender Side:
$n= p*q$
$\varphi (n)=(p-1)*(q-1)$
Let e be original e public key
Let d be the private key
$c= m^e \bmod n$
if c=m then
Locate the public key e at the agreed position in R
Select the secure agreed distance r in the set R
1:   choose alternative public key which is e'
2: compute alternative private key, d' from e'
3: $c' =m^{e'} \bmod n$
4: Attach the agreement piece s to c'
5: Send the block [c',s] to the receiver

Receiver Operation:
1: Extract c from c' by removing s from c'
2: Decrypt c' to get m as following:
$M=c^{d'} \bmod n$
```

IV. Conclusion

In this paper we use a different strong procedure to enhance the security of RSA scheme. This procedure depends on selecting alternative public keys in case of getting an equality of the original message with the ciphetrext. In order to select an alternative public key, the proposed system searches for the nearest secure public key within a set of all valid keys. In addition, this procedure changes the structure of the original ciphertext by salting it with a secure information piece which is safely distributed in house especially for sensitive applications. In the measurement of security, this proposed system uses the diffusion concept of the messages as Shannon states which are one of the enforcement of any cryptographic system. Another important idea in this paper is the agreement among parties to select an alternative public key. This public key is chosen according secure parameters which are the location of the original public key and the distance separated it from one of the subsets of the set of all valid public keys .Finally all sets are protected in a secure repository.

References

[1] Dan Calloway, Introduction to Cryptography and its role in Network Security Principles and Practices. 2009, available at http://www.dancalloway.com/.

[2] R. Rivest, A.Shamir, and L.Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*. 1987; Vol. 21, No. 2, pp. 120-126.

[3] Hinek M. Jason. *On the Security of Some Variants of RSA*, Waterloo, Ontario, Canada: s.n., 2007.

[4] Yang Shuqun. *An algorithm for generating strong primes*, Science and Technology Square, 2006, pp. 74-75.

[5] T.Collins, D. Hopkins, S. Langford, and M. Sabin. 1997, Public Key Cryptographic Apparatus and Method, US Patent 5,848,159.

[6] Peng Jiezhao and Wu Qi. *Research and Implementation of RSA Algorithm in Java*, IEEE, 2008.

[7] W. Mao. *Modern cryptography: theory and practice*, Prentice Hall Professional Technical Reference, 2003, pp. 294 - 296.

[8] Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein. *Introduction algorithms*, MIT press, second edition, 2003.

[9] Sarthak R Patel 1, Prof. Khushbu Shah. Security Enhancement and Speed Monitoring of RSA Algorithm, *IJEDR*. 2014; Volume 2, Issue 2.

[10] Malek Jakob Kakish. ENHANCING THE SECURITY OF THE RSA CRYPTOSYSTEM. *IJRRAS*. 2011; 8 (2).

[11] Gaurav R. Patel, Krunal Panchal, Sarthak R. Pate. A Comprehensive Study on Various Modifications in RSA Algorithm. *NTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH. IJEDR*. 2013; Vol. 1 issue 3.

[12] Sun, Hung - Min, Mu- En Wu, Wei- Chi Ting, and M. Jason Hinek. Dual RSA and its security analysis. *Information Theory, IEEE Transaction*s on 53. 2007; no. 8, 2922 - 2933.

[13] Wang Rui; Chen Ju; Duan Guangwen. A k-RSA algorithm. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, vol., no., pp.21, 24, 27 -29 May 2011.

[14] Garg, V., Rishu, R. Improved Diffie-Hellman Algorithm for Network Security Enhancement. *International Journal of Computer Technology and Applications*. 2012; 3(4).