Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 69 (2014) 22859-22861

ISSN: 2229-712X

Security Enhanced RSA Public Encryption System

Kiran Vedantham*, Moningi Vivek and Ch Ramakrishna Hanish
School of Information Technology, VIT University, Vellore, India.

ARTICLE INFO

Article history:
Received: 16 October 2013;
Received in revised form:
19 March 2014;
Accepted: 29 March 2014;

Keywords
Public,
Encryption.
Cryptosystem.

ABSTRACT

In our paper , we have suggested a variant of the RSA public cryptosystem, it is more effecient than the traditional RSA algorithm which uses the Euler's Totient Function .The discussed RSA variant is very much similar to the traditional RSA. It also is a block cipher like the traditional one but it uses a different Ø(n) function. In the suggested scheme the range of Ø(n) is so high that it increases the security manifold. This makes cryptanalysis very difficult. Methods like brute force attack will fail as the range is very high and such attacks consume a lot of time. We represent Ø(n) as f(n,h) where n can be a Positive Integer(Z). As the value of h keeps increasing the range of values of Ø (n) also keeps increasing exponentially which in turn increases the security exponentially. This is the reason why the proposed scheme can be assumed to be more efficient, reliable and scalable.

Introduction

In the year of 1996, Diffie Helman[2] was the first person who did a research on public key cryptography and present an idea on cryptography that challenged all the researches on the public key cryptosystem that meets the requirements. There were many challenges given likely many algorithms were dated for the public key cryptosystem, out of which one of the most important were RSA algorithm which means Rivert Shelman Adleman algorithm from MIT university who proposed this technique in 1977[3] and it got its name with the initial letters of their surname.

The RSA algorithm is a public key algorithm is a public key cryptography algorithm that is based on difficulty of factoring large integers. Let's describe the RSA algorithm in 3 steps. They are Key generation, Encryption and Decryption. Let us describe each of them in detail. The Key generation of RSA follows the following steps.

Firstly, we have to take the two distinct large prime numbers then take the product of the two prime numbers. Then comes the substitution of heart of algorithm i.e, the Euler totient function. This function is also called as "Ø" function that counts that number of positive integers that are less and equal to n where all the numbers are relatively prime to n. Through which we generate phi function. Then to calculate the value of e such that it should be a random value that lies between one to phi function and should meet the condition that greatest common divisor of e and Ø function should be equal to 1.

Then to calculate the private key exponent that is extension of one important algorithm like Eucledian, exponent algorithm which is the multiplication inverse of modulus of phi function and random integer e.[6] Now second important step is encryption that is taken place by choosing a message as the algorithm is based on the numeric values. So, it should be a value that is in the range of 1 to (n-1) where n is the product of prime numbers. Then calculate the encryption key value, which will be value exponent of random integer e to message and modulus of n then the value is passed for the Decryption which is the third step in which the original message can be retrieved by using modulus by n of exponential of encryption code to the private key exponent which will retrieve the original message.[7] These are the steps that are followed in sequence. In our proposed scheme the phi function will be modified by f(n,h) where h is the positive integers that keeps on increasing. As the h value increases the time complexity increases which increases the security of the algorithm. However out of many public key encryption schemas. The RSA is widely used public key schema which is used for the encryption in digital signature.[1]

Time complexity of algorithm basically describes the amount of time an algorithm takes to run with the given input. It is expressed in big 'O' notation. Security of the algorithm states that how secure is the algorithm. Basically it defines how the algorithm ensures the integrity and encryption with and without any attacks. The time complexity and security are closely related. As the time complexity increases the security of algorithm increases.

Some Security Attacks of RSA:

The security of the algorithm is the key factor in any of the proposed algorithm in the cryptosystem. Some of the security attacks over RSA are stated here when encryption the algorithm in the cryptosystem. Some of the security attacks over RSA are stated here when encrypting the algorithm with lower exponent value that is e value and the smaller value of message then in the decryption the result of exponential message over e will be a small value over product of prime numbers then the cipher text in that case the cypher text message is sent to many people with the same value but each of them took different prime numbers for computation. Then we can decrypt the message easily using the Chinese remainder theorem. Timing attack which was developed by kocher on RSA in 1995[4]. In this attack if the attacker knows the hardware details of any one of the persons who are involving in the conversation and is able to measure the decryption times for several cipher text which are know then they can easily deduce the private key exponent quickly this attack are applied on RSA signature scheme. The other attack is adaptive chosen cipher text attacks which was introduced by Daniel Bleichenbacher in 1998 who described adaption chosen cipher text attack against RSA on encrypted message using padding schema. Another attack on RSA is side channel analysis attack was described using branch prediction analysis. Another attack on RSA is power fault attack[9] that has been discovered

Tele:
E-mail addresses: kiran.ved.09@gmail.com

in 2010 in which the key is recovered by varying CPU power voltage that are taken from the outside limit which cause power failure on server.[5] .

The new attack which is related on fault injection over RSA which was introduced in 1996 by Bonch,de Millo and Lipton. In the year of 1996, Bellocare reaserchers has introduced another type of attack over RSA based on differential fault analysis by attacking the CRT based implementation of RSA.[8].

Public Key Cryptography: RSA Algorithm

Lets see how the traditional RSA cryptography works.

1. Randomly choose any two numbers which are firstly prime and have a huge value so that the cryptanalysis become difficult and let them be p and q.
2. Generate the values of n, q by using n = pq and g = (p-1)(q-1).
3. Now lets choose a random number e such that its value is less than n and gcd both the numbers is 1.
4. Now lets choose a random number d such that its value is less than g and satisfies the equation de=1modg

Basically the value d is used for decryption . The value of d is only with the receiver.

$K_B^+ = (n, e);$

$K_B^- = (n, d);$

The encryption is done using the equation

$C=M^e \bmod n$.(M is the message to be encrypted)

The decryption is done using the equation

$M=C^d \bmod n$ (C is the encrypted message)

The Proposed Scheme

In the proposed scheme we will make RSA expand its boundaries by using an expression other than Φ(n) and we call that expression f(n,h) where h is a randomly selected positive integer value and n is a product of randomly selected two large prime numbers as shown in the example. The best feature of this proposed scheme is that when the value of h=1,then f(n,1) is nothing but Euler's totient function. This means that the proposed scheme is a superset of the traditional RSA cryptosystem. The value of h can go as big as ∞. Below is the proposed algorithm.

Theorem:

Assume that the two randomly selected large numbers are p and q, then their product is represented by n. So n=p*q. Now we calculate f(n,h) which has a similar function as Φ(n), but is a superset of Φ(n) . If f(n,h) is a superset of Φ(n) then, $f(n,h)= (p^h -1)(q^h -1)$. Key generation algorithm To generate the keys entity *A* must do the following: 1. Randomly chooses two large prime numbers *p* and *q* 2. Calculate the value of n after choosing p and q values n=p*q 3. Compute: $f(n,h)= (p^h -1)(q^h -1)$ 4. A random integer I should be chosen in such a way that greatest common divisor (i, f)=1 5. Now calculate the inverse of *d* where $e*d = 1 \bmod n$ 6. Now that we have both the values e, d we can create the Private and the Public key pairs. Private key pair= (n, d) Public key pair= (n, e) Public key encryption algorithm Now here we describe the whole process of how the encryption and decryption takes place. Lets assume that a sender S has to encrypt a message M and send it to the receiver V who has to decrypt the cipher text to read the message content.

Encryption: In this case the sender has to receive the public key generated (n, d) . Keeping the value of n he must calculate f(n,h). From here a random value e is selected such that gcd (e,f)=1. Using the value of e the sender can encrypt the message M to get a cipher text C which is done using: $C=M^e \bmod n$. This cipher text is sent to the receiver through a medium Decryption: Here the receiver tries to decrypt the cipher text using the private key (n, e).This can be done by: $M=C^d \bmod$

Analytics:

The basic analysis discussed here is about the RSA algorithm and our proposed algorithm in the proposed as phi(n,h) as the h value increases the time complexity of the algorithm also increases as the time complexity increases the security of the algorithm increases for an efficient algorithm like RSA the two major factors are given an high priority as the algorithm provides an better efficiency when compared to RSA as the values of h varies .

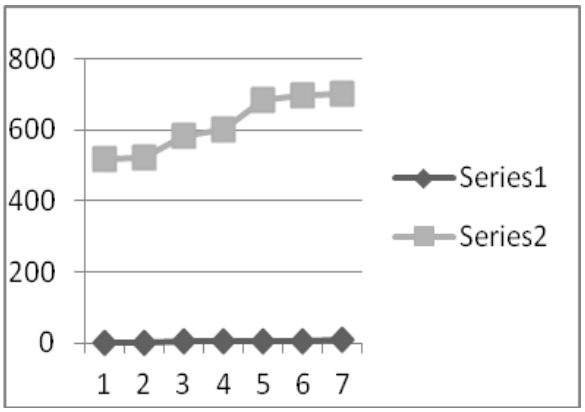

Fig 1 a graph on time complexity verses h values

As we have seen from fig 1 the h values increases the time complexity of the algorithm and basically the security will increase according to our algorithm if h=1 then it will be RSA algorithm the execution time increases slowly so by the above graph we can state that our algorithm has increased efficiency over RSA

Advantages

The main advantage of the proposed variant of RSA algorithm is the range of values of the key e is very high. For instance if we take an example where p=43 and q=47 then n=2021 , Φ(n)= (43-1)(47-1)=1932. Where as the function f(n,h) where say h=2 gives the value $f(n,2)=(43^2-1)(47^2-1)=4080384$.

Thus the proposed scheme gives 4078452 more values than Φ(n) which clearly shows the obvious difference in the ranges. The above advantage makes cryptanalysis by any attacker very difficult as the range is huge and it will take a lot of time to check for each value in that range. This proposed scheme also mitigates any chance of cracking the encryption using methods like Brute Force because of the range which may take a lot of time. This clearly shows that the security has been increased exponentially which is very important in the aspect of any cryptosystem.

2.Clearly the proposed f(n,h) also contains the traditional RSA algorithm in itself. This is obtained when the value of h=1. For example: $f(n,h)= (p^h -1)(q^h -1)$. If we substitute in this equation h=1 we get f(n,h)=(p-1)(q-1) which is the same as ø(*n*). This means that the proposed variant acts as a superset of the traditional RSA algorithm.

Conclusions

In our paper, we suggested an efficient RSA public key encryption system, which is an enhanced version of the original RSA scheme. The proposed RSA scheme is similar to the traditional RSA in the sense that both are block ciphers. How ever in the proposed scheme the Euler totioent function has been replaced by an equation which gives a higher range possibilities for the 'e' value. This depends on the h value wee choose. The

equation is represented by f(n,h). The values of h can be any positive integer. This makes the new variant of RSA more secure, scalable and reliable.

References:

[1]Aboud, S.J.; Al-Fayoumi, M.A.; Al-Fayoumi, M.; Jabbar, H., "An Efficient RSA Public Key Encryption Scheme," *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on* , vol., no., pp.127,130, 7-9 April 2008

[2]Diffie W and Hellman M, "New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976

[3] Rivest R, Shamir A and Adelman L, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communications of the ACM, 21, pp. 120-126, 1978

[4] Remote timing attacks are practical. SSYM'03 Proceedings of the 12th conference on USENIX Security Symposium.

[5]fault based attack on RSA authentication

[6] Aboud, S.J., "An efficient method for attack RSA scheme," *Applications of Digital Information and Web Technologies, 2009. ICADIWT '09. Second International Conference on the* , vol., no., pp.587,591, 4-6 Aug. 2009

[7] Sushma Pradhan, Birendra Kumar Sharma," An Efficient RSA Cryptosystem with BM-PRIME Method", International Journal of Information & Network Security (IJINS) Vol.2, No.1, February 2013, pp. 103~108.

[8] Berzati, A.; Canovas, C.; Goubin, L., "In(security) Against Fault Injection Attacks for CRT-RSA Implementations," *Fault Diagnosis and Tolerance in Cryptography, 2008. FDTC '08. 5th Workshop on* , vol., no., pp.101,107, 10-10 Aug. 2008 [9] Fournaris, A.P.; Koufopavlou, O., "Protecting CRT RSA against Fault and Power Side Channel Attacks," *VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on* , vol., no., pp.159,164, 19-21 Aug. 2012 doi: 10.1109/ ISVLSI.2012.54