Improvement over Public Key Encryption Algorithm for Security in Network Communications

M. Chalapathi Rao[1]

[1]Assoc. Prof. in Department of CSE.Vaageswari College of Engineering, Karimnagar.

Abstract

In this paper we have exhibited the improvement of a public key encryption algorithm which is the development of an effort of RSA. The public key cryptography is a method for encrypting messages to be transmitted over an insecure channel is emerging as fundamental tools for conducting business securely over the internet. Network security is important to the PC users, organizations and the military. With the arrival of an internet security is a big matter; internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing due to that effect different methods have been used to protect the transfer of data, including firewalls and encryption mechanisms. Here we adopted RSA encryption algorithm to give constitutional security by making alterations and appending few other security use of codes in present algorithm.

Key words: RSA Algorithm, Private Key, Public Key, Security, Encryption, Decryption, Cryptosystem.

1. Introduction

The RSA Algorithm was named after Ronald Rivest, Adi Shamir and Leonard Adelman, who first published the algorithm in April, 1977. Since that time, the algorithm has been employed in the most widely-used internet electronic communications encryption program, Pretty Good Privacy (PGP). Encryption is to recipient the security of delicate information. It not only provides the mechanisms in information confidentiality, but is also operated with digital signature, authentication etc. RSA supports multiple key sizes like 128 bits, 256 bits, 512 bits. A massive number and varieties of works have done on the hardware implementation of RSA encryption algorithm. Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data. RSA is probably the most commonly used public key algorithm. It can be used for both for encryption and for digital signatures. Encryption techniques typically use mathematical operations to transform a message into an encrypted form known as cipher text. In the RSA algorithm, the encryption key is the pair of positive integers (e, n) and the decryption key is a pair of positive numbers (d, n). Each user makes the encryption key public, keeping the corresponding decryption key private. To choose the encryption and decryption keys for the RSA algorithm, we first compute as the product of two very large, random prime p and q We then choose d to be a large integer that is relatively prime. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem. In a public key cryptosystem each user places in a public file can encryption procedure E_n. That is, the public file is a directory giving the encryption procedure of each user. The user keeps secret the details of his corresponding decryption procedure D_e. These procedures have the following properties.

I). Deciphering the enciphered form of a message M_{sg} yields M_{sg}. Formally

$$D_e\ (E_n\ (M_{sg}) = M_{sg}$$

II). If a message M_{sg} is first deciphered and then enciphered, M_{sg} is the result. Formally,

$$E_n (D_e (M_{sg}) = M_{sg}$$

Let us start our motivation for the encryption algorithm and its compatibilities in section 2. Then we will give exhibited information about our current work in section 3.RSA public key encryption algorithm shown in section 4. Last section is 5 concludes.

2. Motivation

RSA algorithm has certain parameters that affecting its level of security. By increasing the modulus length plays an important role in increasing the complexity of decomposing it into its factors. This will increase the length of private key and hence difficult to be decrypted without knowing the decryption key. When the length of message is changed then the length of encrypted message will proportionally change, hence larger chunks are selected to obtained larger encrypted message to increase the security of the data in use [1]. RSA -1024 bits is good for last 20 years but now Bern stain described circuitry for fast factorization. It is entirely possible that an organization with suffientely deep pockets can build a large scale version of his circuits and effectively crack an RSA 1024 bit message in a relatively short period of time, which could range anywhere from a number of minutes to some days. We use natural numbers in pair of keys in addition to existing parameters of RSA. Then after simulations of results on basis of speed and security we compare the RSA and new algorithm [2]. We use fast modulation method in RSA for big exponential calculation. RAS Algorithm is based on the exponential, modulus numbers and prime numbers [3]. The plain text block is M_{sg}, cipher text C_{txt} and block size must be less than or equal to $\log_2{}^{(m)}$. The following forms are used for encryption and decryption,

$$C_{txt} = (M_{sg})^{e} \bmod m$$

$$M_{sg}= (C_{txt})^{d} \bmod m$$

Both sender and receiver know the modulus value (m) and encryption (e_n), and decryption exponent (d_e) value is known to any party only even many algorithms are available for public-key cryptography, the RSA algorithm provides more security comparing with many and also it security is far better than other systems. There are some possible approaches to attack RSA algorithm. Some of the important attacks are Brute-force Attacks, Mathematical Attacks and Timing Attacks [4].

3. Literature Review

The RSA algorithm was developed by three professors at MIT, Ron Rivest, Adi Shamir, and Leonard Adelman; their initials give the algorithm its name. This was one of the rst algorithms (mathematical processes) to implement the concept of public-key cryptography [1]. The actual concept of public-key cryptography was discovered by Whitfield Diffie and Martin Hellman just one year earlier. Diffie and Hellman had devised a method that would allow the key to the cryptographic system to be known publicly but still have the system be a secure way to send messages. What they did not know was how to mathematically create one [2]. Rivest, Shamir and Adelman took the concept of Diffie and Hellman and devised a method that uses what is known as a one-way function. A one-way function is a mathematical process that is easy to do one way but is difficult to reverse [3]. The essential requirement of the Public Key Cryptography is that the public and secret keys are mathematically related, but this relationship must be made very hard to determine by an outsider. RSA consume much more encryption time duration in extension to memory expenditure [4]. On the other hand, public key cryptography, as introduced by Diffie et al., is a very powerful technology and seems to be well suited to satisfy the requirements of the global Internet. In fact, it is commonly agreed that this technology is fundamental for a flourishing e commerce and e- business in Internet, and has become the foundation for many such applications. The widespread use of public key cryptography requires a Public Key Infrastructure (PKI) [5]. The aim of the PKI makes sure that a public key in use really reside to the call for entity. Excluding PKI, public key cryptography will not be preferable to conventional private key cryptography. The RSA crypto system is moderated for susceptibility. During no destructive incursion has usually been initiated since years back cryptanalysis of RSA has furnished us a deep awareness into its functionalities, guide lines for better use and implementation. RSA pointed at the latest information security. It doesn’t matter to say that internet security have confidence heavily on the security estate of the RSA cryptosystem [6].

4. Public Key Encryption by RSA Algorithm

4.1 RSA Key Generation

Whoever wants to receive secret messages creates a public key (which is published) and a private key (kept secret). The keys are generated in a way that conceals their construction and makes it 'difficult' to find the private key by only knowing the public key.

We select any two prime numbers

p=17
q=37
n=p*q=629
Ø=576 (Ø = Ø (n) = (p-1). (q-1); needed to determine e and d)
e=5 (arbitrary, but less than n and relatively prime to Ø)
d=461(inverse of e modulo Ø: e. d mod Ø =1)

From these no’s keys are composed

The public key is the pair (e, n)
The private Key is the pair (d, n)

It is 'difficult' to compute d without knowing Ø. It is 'difficult' to factorize n into p. q which is needed for computing Ø

4.2 RSA Encryption

A secret message to any person can be encrypted by his/her public key (that could be officially listed like phone numbers). First of all we need the public key of the person to whom we want to send the message.

Take public key from above formally

(e, n)= (5, 629)

Next we need the message. For simplicity let us demonstrate this here with just one letter to cipher. The letter is “D”. Before we can encrypt this letter we must encode it as a number i.e.

m=4
Encryption itself is m'= 395 (m' = me mod n)

The value m' is the encrypted message sent to the receiver.

4.3 RSA Decryption

Only the person being addressed can easily decrypt the secret message using the private key. First of all we need the private key of the person who got the encrypted message.

Take private key from above formally

(d, n)= (461, 629)

Next we need the encrypted message: Take encrypted message from above

m'= 395
Decryption itself is m=4 (m = m'd mod n)

The Decoded message should match with the above chosen letter “D”.

5. Conclusion

As per the above study it is arrival that RSA algorithm has the equal attention as of the system in the cryptography over network security. By reason of RSA provides the authentication, confidentiality and privateness to entire system. So it is totally build upon the two large prime numbers these can hide your secretes. Consistently we used math of the methods in calculation and added complexity in use of codes for drastic protection.

.

References

[1] SCHNEIER, B., 1996. Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons.
[2] Deng Y., Mao Z., and Ye Y.,. 1998. Implementation of RSA Crypto-Processor Based on Montgomery Algorithm.
[3] Zhang. C.N, Xu. Y and Wu. C., 1997. A Bit-Serial Systolic Algorithm and VLSI Implementation for RSA.
[4] Hinek. M., 2010. Cryptanalysis of RSA and Its Variants.

[5] Rivest, R., Shamir, A., and Adleman, L, 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM.

[6] Stallings W.2003, Cryptography and Network Security: Principles and Practices.

[7] Burnett S. and Paine S, 2001. RSA Security's Official Guide to Cryptography. McGraw-Hill.

[8] Ashenden P. and Lewis J, 2006. The Designer's Guide to VHDL. Morgan Kaufmann Publishers.

[9] Hwang E. Digital Logic and Microprocessor Design with VHDL.

[10] Nedjah.N and Mourelle L.2002.Two Hardware Implementation for the Montgomery Modular Multiplication: Sequential versus Parallel. IEEE.

[11] RSA algorithm using modified subset sum cryptosystem, Sonal Sharma, Computer and Communication Technology (ICCCT), pp-457-461, IEEE 2011.

[12] The large prime numbers based on genetic algorithm, hang Qing, (ICISIE) pp-434-437, IEEE 2011.

[13] An advanced secure (t, n) threshold proxy signature scheme based on RSA cryptosystem for known signers, Kumar, R, Dept. of Compute. Sci. and Eng, pp 293-298, IEEE 2010.

[14] An efficient decryption method for RSA cryptosystem, Ren-Junn Hwang, Dept. of Compute. Sci. and Inf. Eng, pp-585-590, IEEE 2005.

[15] A new RSA cryptosystem hardware design based on Montgomery's algorithm, Ching Chao Yang, Dept. of Electron. Eng, pp- 908-913, IEEE 1998.

[16] A systolic RSA public key cryptosystem, Po – Song Chen, Dept. of Electron. Eng, pp 408-411, IEEE 1996.

[17] Blocking method for RSA cryptosystem without expanding cipher length, NEC Corp, Kanagawa, Japan, pp 773-774, IEEE 1989.

[18] A method for obtaining digital signatures and public key cryptosystems, R.Rivest, A.Shamir and L.Adleman "communication of the association for computing machinery " 1978, pp 120-126.

[19] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory IT-22, no. 6, 1976, pp644-654.

[20] Tatsuaki Okamoto and Shigenori Uchiyama, "A new public key cryptosystem as secure as factoring", Lecture notes in Computer Science 1403 (1998), 308-318.MR1729059.

[21] Richard Crandall and Carl Pomerance, "Prime Numbers A Computational (Second Edition)", pp. 83-113 and pp 173-179 and pp 225-227, Springer ISBN-10:0-387-25282-7,NewYork(2005).

[22] Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. (October 1996). Handbook of Applied Cryptography. CRC Press. ISBN 0-8493-8523-7.

[23] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2001). Introduction to Algorithms (2e ed.). MIT Press and McGraw-Hill. pp. 881–887.ISBN 0-262-03293-7.