INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Implementation of Modified RSA in MATLAB

Ankita Nag
B. E. (Electronics and Telecom.), Pursuing M.E. (Comm.)**,** SSGI, Bhilai, Chhattisgarh, India
Vinay Kumar Jain
Associate Professor, SSGI Bhilai, Chhattisgarh, India

Abstract:
In this Cyber age almost every communication is done through computers via different interconnected networks and over internet. This communication involves simple chatting to e-mails, business over internet, e-commerce. These involve useful data but also financial and personal data. Financial and personal data needs security. For this different security mechanisms developed. One is to make data unreadable. The various cryptographic techniques are private key cryptography e.g. DES, public key cryptography e.g. RSA. The RSA is the most popular public key cryptographic algorithm. In this paper RSA is modified using pseudo random number and implemented in MATLAB. RSA involves complex and intensive computation.And MATLAB is known software package for high performance numerical computation and visualization.

Keywords: *RSA, MATLAB, public key cryptography, public key, private key, prime number*

1. Introduction

The RSA algorithm is an asymmetric key cryptography. Based on the theoretical frame work of Deffie and Hellman in 1977, Ron Rivest, Adi Shamir, Len Adleman at MIT developed the first major asymmetric key cryptography and published their results in 1978. It is named after their first letter of their surnames.Even today, RSA is the most widely accepted public key solution. It solves the problem of key agreements and distribution.[1]. In RSAthere are two keys one for encryption - a private or secret key and a public key for decryption.If one encryption key is used for encryption the only corresponding key must be used for decryption.The beauty of the scheme is that every communicating party needs just a key pair with any number of other communication parties. Once someone obtains a key pair she can communicate with anyone else. Secret is kept completely secret and public key is made publicly known to communicating parties. Sender sends the message encrypting it with the public key of receiver. Receiver receives the message by decrypting it with the corresponding private key. RSA is a block cipher. In block cipher the plain text to be encrypted is first taken in blocks .Then this block is encrypted. RSA has stronger security than single key cryptography. It is based on the mathematical fact that to find the product of two large bit prime numbers is easier but the factorization of their product is extremely difficult. Prime numbers are those numbers which have no common factor other than 1. In this paper, MATLAB is used to perform the intensive calculation to implement the RSA algorithm.

The term MATLAB stands for 'MATrixLABoratory'. As the name suggests MATLAB does all the calculation in matrix form or in array.

1.1. Methodology of RSA

Here p and q are two large bit prime numbers say 512 bits. And e and d represents encryption or public key and decryption key or private key respectively.

1. Select two large bit prime numbers p and q.
2. Calculate n = p x q.
3. Calculate z = (p-1) x (q-1)
4. Select encryption key e : 0 <e< n
5. Select the private key (i. e. decryption key), d such that ed mod z = 1
6. Publish public key- {e,n}
7. Keep private key secret {d,p,q}
8. Encryption -Cipher Text, C = M^e mod n
9. Decryption - Plain Text, M = C^d mod n

The real challenge lies in selecting the two large bit prime numbers p and q. Their product must give larger bit number**n**. This larger bit number must be tough to factorize. The larger the bit tougher the factorization. This tough factorization is the strength of RSA.

Increasing bits definitely increases security of RSA Algorithm but is slows the encryption and decryption process. So it is generally used in SSL for key exchange not for each message exchange since it is 1000 times slower than symmetric key e.g. DES. It is used for secure exchange of symmetric key between web client and web server

This paper is organized as follows: Section II past work related to the project and experimental result of classical RSA Section III describesthe proposed algorithm, Section IVdescribes theModified RSA.RSA is modified by embedding the encrypted data or cypher with pseudo random number. Finallysection V concludes the work.

2. Past Work Related to the Project

In the reference paper "Improving the SSL using RSA algorithm" introduces the idea of bit stuffing in the classical RSA. In the paper RSA algorithm is modified to make it tougher to interpret even after it is disclosed by the intruder using the private key. In this way authors explain how modified RSA can provide more security to Secure Socket Layer since Secure Socket Layer SSL Protocoluses RSA algorithm for key exchange.In this way SSL providesauthentication and integrity to the message. So the message is protected against its misuse by the attacker. It is very important to ensure security of message after implementation of General Number Field Sieve (GNFS) on 512 bit RSA Algorithm successfully. He can delay or modify information, creating misunderstanding between the communicating parties if the message is not protected. The GNFS algorithm isused to factorize n, where n is the multiplication of two large prime numbers p and q. It iscomputed by distributing the result over large number of computers. [6].For making RSA more secure its bit is increased to 2048 bits at present.So the conclusion is increasing the number of bits is considered as a measure to obtain security increasing its processing time at the same time shown in experimental results below:

2.1. Experimental Results of Classical RSA

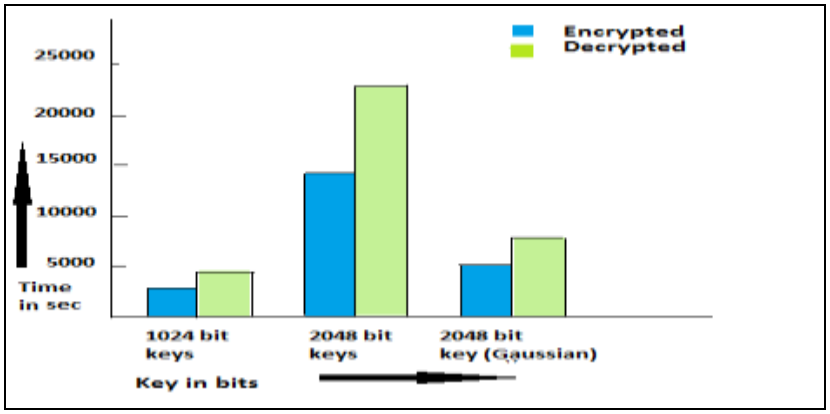

Figure 1: Time for Encryption and Decryption

In this section, the authors have compared and evaluated the classical and the modified authentication functions of SSL [12] by showing the run time results of three different examples for the 1024 bit key and the 2048 bit key generated using two prime numbers having 512 bit keys each and 2048 bit key generated using two prime numbers each with 512 bit keys (In this they have used Gaussian Integer).

These are based on tested examples on messages and the corresponding results are shown in the above. And it is concluded that while encryption and decryption using 2048 in the domain of integer is 6times greater than the one uses 1024 bits. [12]

L. Scripcariu, M.D. Frunze [4] was commencing some weak points of RSA algorithm and proposed a method for secure public key. The main concept of this paper is for encryption *(e, N)* change every time public key for encryption.[2]. Thus the authors also gave concept for making RSA algorithm more secure.

3. Proposed Algorithm

In the paper pseudo random number is added to the encrypted text or cipher. It is for the purpose that if the message is intercepted somehow it is still unreadableto the intruder. The idea behind this paper is to modify the RSA key from 512 bits to 512 bits by applying BITSTUFFING instead of ordinary integers using the same prime numbers used by the 512 bits.[8] Inthis way modified RSA ensures more security.

The following is the proposed diagram for this modifies communication which we designed.

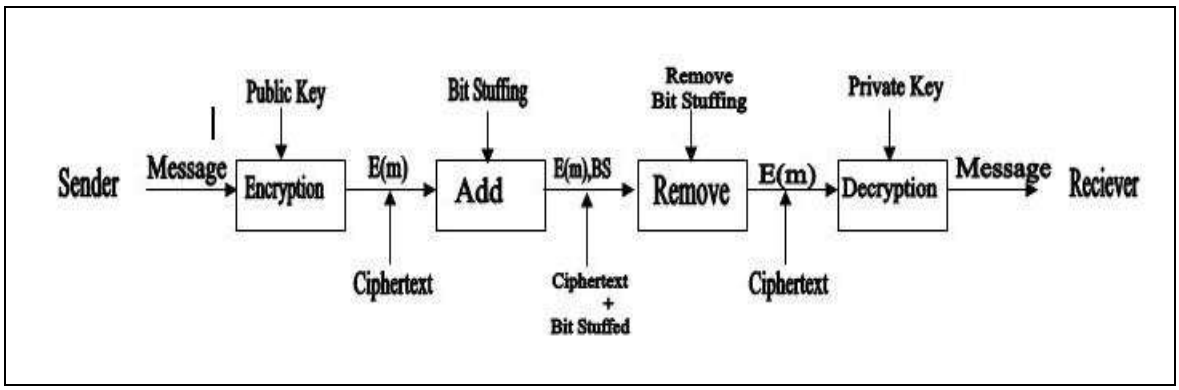

Figure 2: Encryption and Decryption

From this diagram it is clear that the communication which will occur will be secure because the decryption key is not sharedand is only known to the receiver as follows:

In data transmission and telecommunication, bit stuffing is the insertion of non-information bitsinto data. Stuffed bits should not be confused with overhead bits [8].So the modified RSA can be for key exchange in SSL to enhance its security.
Modified RSA is also a good option against increasing number of bits in keys for security purpose as it take less time and energy to encrypt and decrypt the message or plain text as compared to using keys of increased number of bits.
Appending pseudo random number technique has been used for frame synchronization in communication system so modified RSA will provide good synchronization.
Synchronizing bit rates or to fill buffers or frames
Appending pseudo random number technique can be used. Bit stuffing maybe used to synchronize several channels before multiplexing or to rate-match two single channelsto each other.[14]Here appended bits is not part of message but its only purpose is security.

4. Methodology of Improvedrsa

Here p and q are two large bit prime numbers say 512 bits.

1. Select two large bit prime numbers p and q.
2. Calculate n = p x q.
3. Calculate z = (p-1) x (q-1)
4. Select encryption key e : 0 <e< n
5. Select the private key (i. e. decryption key), d such that ed mod z = 1
6. Publish public key- {e, n}
7. Keep private key secret {d, p, q}
8. Encryption -Cipher Text, C = M^e mod n
9. Appending bits, C1 = [C Appended bits]
10. At Receiver, appended bits are removed
    C = [C]
11. Decryption - Plain Text, M = C^d mod n

5. Conclusion

The message is successfully encrypted, appended with pseudo numbergenerated by pseudo number generator and sent to the receiver.At the receiver the appended bit is removed. Then the message is decrypted to obtain the plain text. We can also sketch the graph of original message against cipher to deduce how change in plain text affects change in cipher.

6. References

1. AtulKahate, Cryptography and Network Security, Tata McGraw-Hill Education, 2003
2. B. R. Ambedkarand S SBedi "A New Factorization Method to Factorize RSA Public Key Encryption " Department of CS and IT, MJP Rohilkhand University, UP, IndiaIJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011
3. A. J. Kenneth, P. C. Van Orshot and S. A. Vanstone, Handbook of applied Cryptography, CRC press, 1977.
4. L. Scripcariu, M.D. Frunza, "A New Character Encryption Algorithm", ICMCS 2005, pp. 83 - 86, Sept., 2005.
5. RSA website, 5.1 Security on the Internet, http://www.emc.com/security/rsa-securid/rsaauthentication-manager.htm
6. IT security web site, the risks of short RSA keys for secure communications using SSL, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4259828&url=http%3A%2F%2Fieeexplore.ie ee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4259828
7. H. Otrok, Security testing and evaluation of Cryptographic Algorithms, M.S. Thesis, Lebanese American University, June 2003.
8. Bit-Stuffing http://en.wikipedia.org/wiki/Bit_stuffing
9. Cisco Systems, Introduction to Secure Sockets Layer, http://www.ehacking.net/2011/05/securesockets-layer-ssl-introduction.html
10. A. 0. Freier, P. Karlton and P. C. Kocher, The SSL Protocol, version 3.0, http://www.cryptoheaven.com/Security/Presentation/SSL-protocol.htm
11. W. Stallings, Cryptography and Network Security, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1999.
12. H. Otrok, PhD student, ECE Department, Concordia University, Montreal, QC, Canada and R. Haraty, Assistant Dean, School of Arts and Sciences, Lebanese American University, Beirut, Lebanon and A. N. El-Kassar, Full Professor, Mathematics Department, Beirut Arab University,Beirut, Lebanon "Improving the Secure Socket Layer Protocol by modifying its Authenticationfunctions" 2006
13. RudraPratap, Getting started with MATLAB, Oxford University Press, 2010Impact of Secure Socket Layer on Internet Servers" 2000
14. Purshotam,Dept. of Computer Engineering, Lovely Professional University, Punjab and RupinderCheema, PEC University of Technology, Chandigarh and AyushGulati, Lovely Professional University, Punjab ," Improving the Secure Socket Layer using modifying RSA algorithm"2012