International Journal of Latest Research in Science and Technology **ISSN (Online):2278-5299**
Vol.1,Issue 3 :Page No.225-228 ,September-October 2012
https://www.mnkpublication.com/journal/ijlrst/index.php

IMPLEMENTING SECURE SOCKET LAYER BY USING LBC-PUBLIC KEY ALGORITHM

[1]**Prakash Kuppuswamy**, [2] **Prof. Osama Amer,** [3] **Peer Mohamed Appa**
[1]Lecturer, Department of Computer Engineering & Networks, Jazan University, KSA
varshiniprakash@rediffmail.com, kpmvellore@yahoomail.com
[2] Professor, Department of Computer Engineering & Networks, Jazan University, KSA
[3]Lecturer, Department of Computer Science, Jazan University, KSA Peer_cse@yahoo.co.in

Abstract- **The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications to provide application-independent secure communication over the Internet for protocols such as the Hypertext Transfer Protocol (HTTP). The SSL protocol is intended to provide a practical, application-layer, widely applicable connection oriented mechanism for Internet client/server communications security. This paper gives a detailed technical analysis of the cryptographic strength of the SSL protocol. It is a cryptographic protocol which has been used broadly for making secure connection to a web server. SSL relies upon the use of dependent cryptographic functions to perform a secure connection. The first function is the authentication function which facilitates the client to identify the server and vice versa. There have been used, several other functions such as encryption and integrity for the imbuement of security. The most common cryptographic algorithm used for ensuring security is RSA. It still has got several security breaches that need to be dealt with. An improvement over this has been implemented in this paper. In this paper, a LBC has been proposed that switches from the domain of integers to the domain of bit stuffing to be applied to the first function of SSL that would give more secure communication. The introduction of bit stuffing will complicate the access to the message even after getting the access to the private key. So, it will enhance the security which is the inevitable requirement for the design of cryptographic protocols for secure communication.**

Keywords-*Secure Socket Layer (SSL), Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA), Linear Block Cipher(LBC), Plain Text (PT), Cipher Text (CT), Bit Stuffing, TCP, HTTP*

I. INTRODUCTION

The communication medium that involves a lot of transmissions of data travelling back and forth, the protocol plays an important role in making this communication possible. Most transaction systems read information passed into it from the purchasing server's buyer interface application. It then generates some kind of message format or structure. This formatted data stream is then transmitted to the seller. At the seller's site, the data is fed into the transaction system which maps the standard fields into the simple file needed by the receiving computer application, edits and verifies the incoming information, and then passes it to the receiving order entry application for processing.[4]

The Secure Socket Layer protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions. SSL is designed to make use of TCP to provide a reliable end-to-end secure service. It secures the communication by providing message Encryption, Integrity, and Authentication. The SSL standard allows the concerned components to negotiate the encryption, authentication, and integrity mechanisms to use. [6]

- *Encryption* is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to 'decrypt' it to obtain the original message.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Authentication:* The process of proving one's identity. [5]

Authentication is the first function found in SSL. Its goal is to perform identification and authentication of the parties involved in the communication. Authentication is achieved using public key encryption and a digital certificate issued by the trusted Certificate Authority [7].

II. PREVIOUS WORK

Several research papers have been presented discussing security aspects of SSL. Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. SSL protects the communication between a client and a server and provides authentication to both parties to secure communication. SSL provides point to point security. SSL is divided into two layers, with each layer using services provided by a lower layer and providing functionality to higher layers. The SSL record layer provides confidentiality, authenticity, and replay protection over a connection-oriented reliable transport protocol such as TCP. Layered above the record layer is the SSL handshake protocol, a key exchange protocol which initializes and synchronizes cryptographic state at the two endpoints. After the key-exchange protocol completes, sensitive application data can be sent via the SSL record layer.[8]

In the following review, different methods were used in order Securing SSL. **H. Otrok, R.Haraty, and A. N. El-**

Publication History
Manuscript Received : 29 September 2012
Manuscript Accepted : 12 October 2012
Revision Received : 19 October 2012
Manuscript Published : 31 October 2012

Kassarm (2006), proposed "Improving the Secure Socket Layer Protocol by modifying its Authentication functions". The most common cryptographic algorithm used in this phase is the RSA algorithm. The second function is confidentiality that is used to keep the communication confidential. It uses symmetric cryptography to exchange messages confidentially. Integrity is the last function used to ensure the integrity of the data against snooping. This is performed using message digests. Checksum of the message is used for message digest.[2]

Also Parshotam, Rupinder Cheema and Aayush Gulati (2012), " Improving the Secure Socket Layer by Modifying the RSA Algorithm". In this research they present the modified version of RSA in the BIT STUFFING RSA. The idea behind this paper is to modify the RSA key from 512 bits to 512 bits by applying BIT STUFFING instead of ordinary integers using the same prime numbers used by the 512 bits. In this way we are making SSL more secure by using 512 bits and 512 bits for prime numbers. Confidentiality is the second function used in SSL. The proposed method entirely based on RSA algorithm and it appends the BIT STUFF. The security of SSL relies on RSA, moreover appending BIT STUFF is not more feasible solution in usage.[1]

Also A. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol, version 3.0". The RSA used in SSL depends on the integer arithmetic. In order to generate a key with size 512 bits we need two distinct primes each with 256 bits size. 512 bits is equivalent to 155 decimal digits. The standard RSA Algorithm used for authentication is as follows:

1) Firstly find two large primes p and q and compute their product n =p x q.
2) Secondly find an integer d that is
3) co-prime to φ (n) = (p-1)(q -1).
4) Compute e from e d≡ l mod (p-1) (q-1).
5) Then broadcast the public key, which is the pair of numbers (e, n).
6) Message to be transmitted, that is m, say as a sequence of integers {m} each in the range 1 to n.
7) Now encrypt each message, m, using the public key by applying the rule C= m^e(mod n).
8) The receiver will decrypts the message using the rule m = C^d (mod n).

III. PROPOSED SCHEME

Here, we introduce our LBC algorithm with BIT STUFF multiplication is giving more secure to the SSL protocol. In the following section, we will briefly present the LBC algorithm in the BIT STUFFING. The idea behind this paper is to modify the RSA key from 512 bits to 512 bits by applying BIT STUFFING using multiplication instead of appending the numbers or using the same prime numbers used by the 512 bits. In this way we are making SSL more secure by using 512 bits and 512 bits for prime numbers.

The following is the proposed diagram for this modifies communication which we designed. From this diagram it is clear that the communication which will occur will be secure because of the keys are only known to the sender and receiver as follows

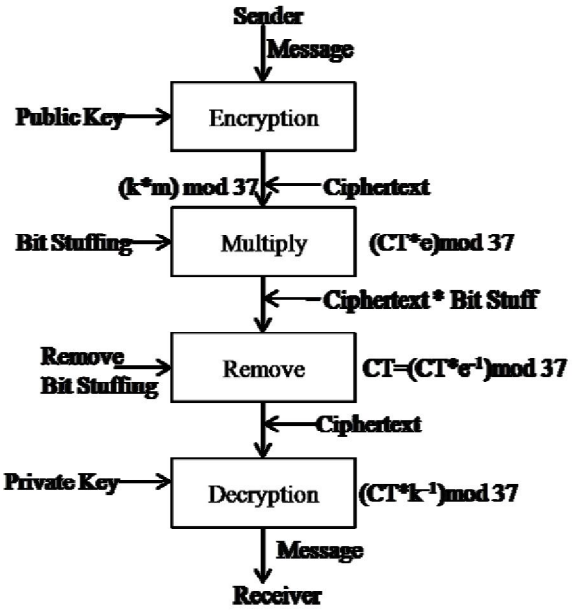

Fig. 1 LBC Structure

In data transmission and telecommunication, bit stuffing is the insertion of non-information bits into data. Stuffed bits should not be confused with overhead bits [8]. Bit stuffing is used for various purposes, such as for bringing bit streams that do not necessarily have the same or rationally related bit rates up to a common rate, or to fill buffers or frames. The location of the stuffing bits is communicated to the receiving end of the data link, where these extra bits are removed to return the bit streams to their original bit rates or form. In this LBC method Bit stuffing also we are making very strong and secure using multiplication of random variable. Like these extra bits will confused to the unauthorised entities and then unauthorised person will not determine the extra bits because only the authorized person will know which extra bits are used in the encryption method.

The domain BIT STUFFING was proposed that this modification is reliable and more secure than the classical RSA and previous case study.

Step 1: Select invertible matrix, It is a key of the algorithm

Step 2: 'k' should be giving the result of $k*k^{-1}$ mod 37 = 1

Step 3: Now make the transpose selected message

Step 4: Multiply 'k' matrix with message.

Step 5: Select 'e'(BIT STUFF) any number and multiply with calculated message (m *BS)

Step 6: Find the modulo 37 from calculated message, the remainder value is called Cipher text.

Step 7: After received Cipher text calculate with and e^{-1} and mod 37 (Removing BIT STUFF)

Step 8: Calculate with cipher text using k^{-1} mod 37

Step 9: The remainder value is called Plain Text. PT=(CT*k^{-1})mod 37

IV. EXPERIMENT & RESULT ANALYSIS

In the case study we have took an one general example and performed the operation by using the Algorithm.

Step 1: First we have to select invertible matrix say as k

$$\begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix}$$

Step 2: 'k' should be giving the result of $k*k^{-1}$ mod 37 = 1

(2 * 5) – (1 *4) = 6 i.e (6*6) mod 37 = 1 and k^{-1} =C_{11} [-1]1+1 x [5] = [-1]2 x [4] = 5

C_{12} [-1]1+2 x [4] = [-1]3 x [3] = -4

C_{21} [-1]2+1 x [1] = [-1]3 x [1] = -1

C_{22} [-1]2+2 x [2] = [-1]4 x [2] = 2

$$\begin{pmatrix} 5 & -1 \\ -4 & 2 \end{pmatrix}$$

Step 3: Make the transpose of given message as (9,14)

Step 4: Multiply 'k' matrix with message.

$$\begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix} * \begin{pmatrix} 9 \\ 14 \end{pmatrix} \text{ mod } 37 = (32, 32)$$

Step 5: Select 'e'(BIT STUFF) any number and multiply with calculated message (m *BS)

Assume here we selected 3 and multiplied with (32,32) = (96,96)

Step 6: Find modulo 37 from calculated message, the remainder value is called Cipher text.

96 mod 37 = 22. Therefore After multiplying message with BIT STUFF block is (22,22).

Step 7: After received Cipher text calculate with and e^{-1} and mod 37 (Removing BIT STUFF)

Now inverse of 3 = 25 verify (3 * 25)mod 37 =1

Multiply with (22 * 25) mod 37= 32.

Therefore After removing BIT STUFF the message block value is (32,32)

Step 8: Calculate with cipher text using k^{-1} mod 37

Now use inverse of the linear matrix with (32,32)

Step 9: The remainder value is called Plain Text. PT=(CT*k^{-1})mod 37 then (416, 1568) mod 37 =(9, 14)

This way we can easily encrypt and decrypt the message and can secure the communication

The security and performance of methods are primitives and protocols can be evaluated under several different models. Here we present a performance comparison between LBC algorithm and other existing algorithm. Here we are examining two types of facts for consideration of performance. First one is computational performance and second one is communication performance. Computational performance refers to the speed of computation required to perform cryptographic operations. Communication performance indicates the total security required for transmission of data between two parties.

TABLE I Character Processing Performance

	No of Characters	Performance
RSA	10	10 Times
MODIFIED RSA[1]	10	10 Times
PROPOSED-LBC	10	5 Times (2 letter each block

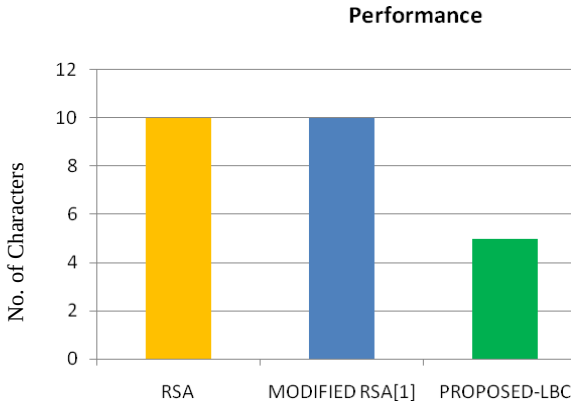

Fig. 2 Character Processing Analysis

V. CONCLUSION

In this paper we have proposed a framework for securing the communication between the client and the server in SSL. The RSA algorithm modified RSA bit stuffing algorithm has got several vulnerabilities that may be exploited, thus facilitating hacking of the algorithm. So, there is a need for devising security mechanisms for the same to thwart the exploited breaches. In this paper, LBC algorithm has been implemented which incorporates the use of bit stuffing on multiplication basis. This mechanisms being followed will enhance the security as the generated number will not be repeated. Moreover, as with the implication of this novel algorithm, intruders irrespective of having access to the private will not be able to access the message as knowledge of bit stuffing is too required prior to accessing the message. So, this enhanced the security of the algorithm thus widening its domain of trusted usage.

VI. ACKNOWLEDGEMENT

We would like thank to Dean Dr. Omar Saeed Mushayt and Vice Dean Dr. Saeed, Jazan University, KSA and Dr.Wajeb Gharibi-Associate Professor & Chairperson of Department of Computer Engineering Networks for their extreme support in the entire manner.

REFERENCES

[1] Parshotam, Rupinder Cheema and Aayush Gulati *"Improving the Secure Socket Layer by Modifying the RSA Algorithm*" International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, June 2012.

[2] H. Otrok, R.Haraty and A. N. El-Kassar, *"Improving the Secure Socket Layer Protocol by modifying its Authentication functions"* 2006.

[3] A. 0. Freier, P.Karlton and P.C.Kocher, *"The SSL Protocol, version 3.0"*, www.cryptoheaven.com.

[4] Judy Nguyen, *"An analysis and comparison of E-commerce Transaction Protocols-purchasing order"*, 1999 SJSU.

[5] A. Menezes, P. vanOorschot, and S. Vanstone, *"Handbook of Applied Cryptography"*, by, CRC Press, 1996.

[6] http://docs.oracle.com/cd/E17904_01/core.1111/e10105/ sslconfig.htm

[7] RSA website, *Security on the Internet*, http://www.emc.com/security/rsa-securid/rsaauthentication-manager html

[8] H.Otrok, "*Security testing and evaluation of Cryptographic Algorithms*", Lebanese American University, June 2003.

[9] Yogesh Joshi, Debabrata Das, Subir Saha, *" Mitigating Man in the Middle Attack over Secure Sockets Layer"* International Institute of Information Technology, Bangalore, India, 2009.

[10] A. J. Kenneth, P. C. Van Orshot and S. A. Vanstone, "*Handbook of applied Cryptography"*, CRC press, 1977.

[11] W.Stallings, *"Cryptography and Network Security*", 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1999.

Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar proceeding in 'Dravidian University'. He has been published few journals/Technical papers and participated many international conference in Rep. of Maldives, Libya and Ethiopia. His research area Cryptography, Bio-informatics, Network algorithms etc.,

Prof. Osama Amer is working as a Professor in Department of Computer Engineering & Networks, College of Computer Science & Information Systems, Jazan University, Jazan, Kingdom of Saudi Arabia. Visiting Professor-Research Institute of Electronics, Shizouka University,Japan and Faculty of Engineering, Bahrain University,Eissa Town – Manama. He is senior member of IEEE-USA, ICE-Japan. His research interests include Information Security, Design & analysis of network algorithms.

Peer Mohamed Appa Lecturer, Computer Science Department in Jazan University, KSA. He has been published few journals/Technical papers and participated many national and international conference. His research area Cryptography, Bio-informatics, Image processing etc.,