Contemporary Engineering Sciences, Vol. 7, 2014, no. 20, 947 - 956
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.48115

SSL/TLS Record Protocol Based on the Triple DES-96 Cryptosystem

P. D. Filio-Aguilar

Universidad Autónoma del Estado de México
Hermenegildo Galeana No. 3 Col. María Isabel,
Valle de Chalco. C.P. 56615 Edo. de México

R. Flores-Carapia

Instituto Politécnico Nacional, CIDETEC
Av."Juan de Dios Bátiz" s/n esq. Miguel Othón
de Mendizábal, Col. Nueva Industrial Vallejo, Del. Gustavo
A. Madero, México, D.F., C.P. 07700

V. M. Silva-García

Instituto Politécnico Nacional, CIDETEC
Av."Juan de Dios Bátiz" s/n esq. Miguel Othón
de Mendizábal, Col. Nueva Industrial Vallejo, Del. Gustavo
A. Madero, México, D.F., C.P. 07700

Abstract

Due to the absolute safety needed when sensitive information via the Internet is used, complex algorithms and cryptographic protocols such as SSL/TLS are required. This paper presents a comparison of the Triple DES cipher system that is part of the suite of encryption SSL/TLS and the cryptographic system Triple DES-96 having the following differences: Triple DES-96 begins with an information block of 96 bits, and Triple DES with a 64 block bits, besides, Triple DES-96 takes a variable permutation PV from the Triple DES keys and the number e is calculated. Furthermore, the expansion table E moves to the output

of S Boxes making it possible to combine with the permutation P and perform in a single instruction at run time.

Keywords: Triple DES, Triple-DES-96, Transcendental numbers, SSL/TLS Record Protocol, Variable permutations

1 Introduction

Initially computer networks were used to exchange e-mail and facilitate the printing of documents, so security did not require special attention. Today millions of people use these networks for; banking, online shopping, tax, e-commerce and exchange of personal information [10].

However, along with these great benefits offered by networks are significant risks. Servers can be substituted, financial transactions could be counterfeit, the identity of a user can be spoofed, private information could be disclosed, firewalls and networks of a company can be violated and sabotaged [9].

That is why complex cryptographic algorithms have been designed, which are a set of techniques that protect or verify information in particular, through the use of keys and are constantly analyzed by mathematicians and cryptographers. The constant research and study of these cryptographic algorithms result in the development of protocols such as SSL (Secure Sockets Layer) [2] created by the company Netscape and its successor TLS (Transport Layer Security) [15] standardized by the IETF [16], which make use of digital certificates and cryptographic sets to establish privacy and secure communications over the Internet, for trustworthy of personal information [6].

These protocols allow client-server applications to communicate in a way designed to prevent falsification of sender identity and the integrity of the message. Hiding data through cryptographic methods while browsing secure sites and their uses are given in electronic commerce, online banking, network security, authentication and data encryption [3].

Cryptographic algorithms under SSL/TLS are: RC4, DES, Triple DES, AES, RC2, IDEA and Fortezza, RSA, Diffie-Hellman, MD5 and SHA-1 [4]. This paper analyzes the Triple DES-96 cryptographic system, and proposes its inclusion in the encryption protocol SSL/TLS, which will permit the encrypted data to be performed in less time.

2 Preliminaries

2.1 Data Encryption Standard (DES)

DES is a symmetric encryption algorithm [8] that was approved by the American National Standards Institute (ANSI) in 1973 and as a Federal Standard

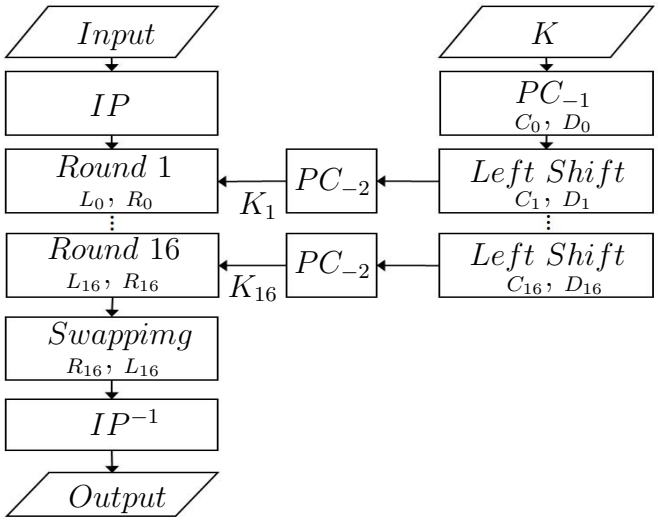

Figure 1: DES Algorithm

FIPS in 1977 [7].

The algorithm uses the encryption by blocks that break the original message into strings of 64 bits length, equivalent to eight symbols in ASCII [13]. In this process the block input also known as input or plaintext is followed by an initial permutation IP and its division into two blocks of 32 bits L_0 and R_0, in function of K whose length is 56 bits, which undergoes a process of permutations. This operation is known as round and this process is applied 16 times on the plaintext, the same operations in which the information is combined with the 16 sub keys generated from K. In the last round the two resulting halves L_15 and R_15, back together and pass through the inverse permutation P^{-1} to produce an output of 64 bits, known as the cipher text. Finally, the decipher process for the encrypted message merely does it in reverse. A schematic of this operation is shown in Figure 1.

2.2 Triple DES

In 1998, using a machine called "DES Cracker" the EFF (Electronic Frontier Foundation) broke the DES encryption with a brute force to test all possible keys [12]. Then a 56-bit key was no longer sufficient to avoid such attack, this gave birth to Triple DES.

Triple DES performs DES procedure, but this is repeated three times in the Encrypt-Decrypt-Encrypt form (EDE), has three keys K_1, K_2 and K_3 of 64 bits each, of which K_1 and K_2 must be different. Data is encrypted with K_1 decrypted with K_2 and finally encrypted again with K_1. This last step can use a different key K_3 [20].

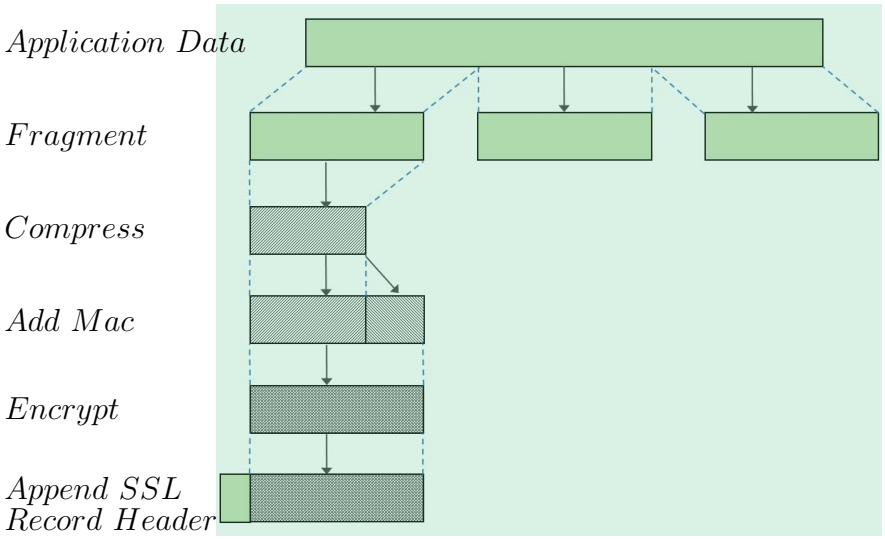

Figure 2: SSL/TLS Record Protocol Operation [19]

If $K_(1) = K_3$ is used the complexity of Triple DES is $2^1 12$ and if the three keys are different then the complexity is 2^{168}. Therefore currently brute force attacks are not possible. However, due to a larger key length being used, it takes longer to perform Triple DES cryptographic operations which are reflected in the execution time, so it is considered a slow algorithm [5].

2.3 SSL/TLS Record Protocol

This protocol specifies how to encapsulate the data transmitted and received. First data is fragmented into manageable blocks, optionally compresses, calculates and applies a message authentication code (MAC). This fragment is added to generate a data packet which is encrypted using symmetric cryptography and then a Header Record is added (type and content length, and the version of SSL/TLS). Then the resulting blocks are transmitted. This operation is illustrated in Figure 2. It is worth mentioning that while the algorithms have not agreed in the negotiation phase, records are not encrypted or authenticated, and at that moment algorithms are null [11].

To function, the following cryptographic algorithms are implemented: for key exchange; RSA, Diffie-Hellman, DSA or Fortezza for summary functions or hash; MD5 or SHA any of the family, and for symmetric encryption AES, IDEA, DES, Triple DES and Fortezza.

2.4 Transcendental number e

A transcendental number is one that cannot be obtained by solving an algebraic equation with rational coefficients. This number was first used by the mathematician John Napier, but it was Leonard Euler who discovered many of its properties [1]. The value of e is given by the equation: (1) e = $lim_{n\to\infty}(1 + 1/n)^n$ = 2.71828182845904523536028747135 27 ... is a first approximation to their digits, which are used in this work to develop the variable permutation PV and its inverse PV^{-1}.

3 Proposed Model

Unlike Triple DES that starts with a fixed permutation of a block of 64 bits, Triple-DES-96 begins with a block of 96 bits and a variable permutation applied at the beginning of the first cycle in third round, and its inverse at the beginning of the round of the fifteenth round of the encryption process in the third cycle [18]. The algorithm Triple DES-96 is as follows:

1. The input string is of 96 bits which is divided into two blocks of 48 bits L_i and R_i, the latter will be the XOR operation performed $Input = R_(i) \bigoplus k_i$ where k_i is 48 bits.

2. $Input$ 48-bit value is now the entrance to the $SBoxes$, and 32 bit output will be called C.

3. If applying the permutation P, to C, the result is a string of 32 bits. However, a string of 48 bits is needed for the x-or operation with L_i which is why the permutation E is used and is combined with the permutation P (Figure 3).

Now the chain is defined $f_{96}(R_(i,)k_i) = E(C)$ Triple DES-96 uses three cycles, the first is a DES-96 [14] with the inclusion of variable permutation PV generated from transcendental number e, and it applies in the entrance of the third round (Figure 4). The second cycle is a decryption algorithm DES-96. The third cycle is DES-96 encryption, but at the entrance to the fifteenth round includes PV^{-1} that is applied in the chain L_{14} and R_{14}. Triple DES-96 also uses three keys K_1, K_2 and K_3.

The permutation is calculated according the following procedure: The three keys, K_1, K_2 and K_3 are concatenated to represent an integer number, say l. Then, multiply $l \times e$ is proposed, and using this result, it is possible to find integer positive constants and with these constants build a permutation [17]. After the above considerations, the objective of this work is to include the encryption algorithm Triple DES-96 in the SSL/TLS Record Protocol,

25	16	7	20	21	29
21	29	12	28	17	1
17	1	15	23	26	5
26	5	18	31	10	2
10	2	8	24	14	32
14	32	27	3	9	19
9	19	13	30	6	22
6	22	11	4	25	16

Figure 3: Permutation Resulting from the combination of E and P

77	69	35	8	2	41	75	63	4	70	7	59
82	92	22	16	33	31	47	72	80	6	5	12
40	79	24	36	87	51	17	93	29	81	21	55
57	66	58	74	10	49	1	83	88	44	32	94
90	43	64	85	62	86	78	34	27	15	61	28
84	60	54	20	42	95	68	9	96	19	14	37
18	76	73	25	11	56	65	3	13	52	67	38
71	39	46	45	91	30	50	48	23	26	53	89

Figure 4: Permutation generated from e

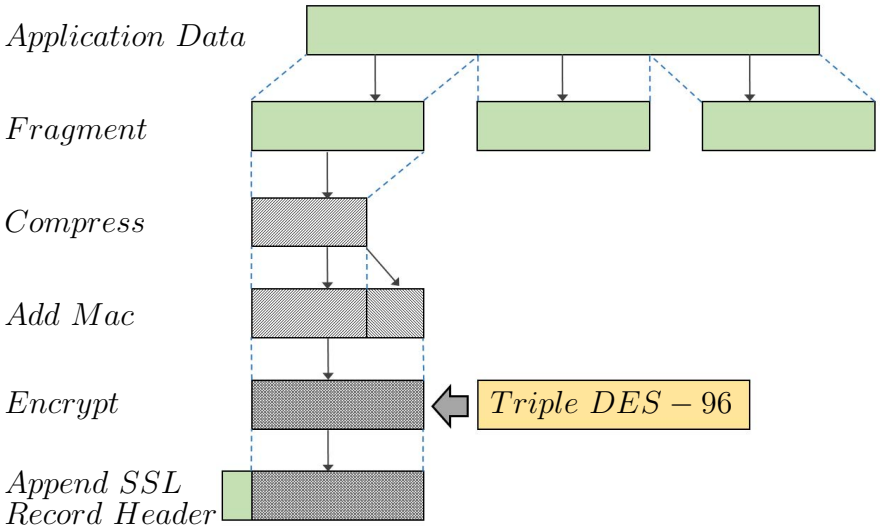

Figure 5: Proposed model

together with the suite of encryption algorithms used for operation, resulting in the following model. Figure 5.

4 Experimental Evaluation

The two algorithms Triple DES and Triple DES-96 were developed in Java programming language version 7 update 60, according to FIPS 46-3 [8] and the next set of keys was used in both cases:

K_1 = 133457799bbcdff1

K_2 = fedcba9876543210

K_3 = 9876542310fedcba

The l = 133457799bbcdff1fedcba98765432109876542310fedcba

The $l \times e$ result, after of decimal point is:

ac448007b928fef05b9c5ce4f95415b1c06d7c47209be29db7ac17689ffb10cadcc
c1473b0fcad04b19ed86b6b2be784952ad4976c06aeee4235228ac9b3005526b0
35b6facf8f8fb92a4d3c328ea924ac8adb45b33a080b40777841e3a1599e.

The permutation is shown in Figure 4.

Each algorithm was run separately, over 1000 files of different types and sizes ranging from 1KB to 254MB. Tests were performed on a machine with Intel Core2 Duo 3.00 GHz processor, 4 GB of RAM, running 32 bit Windows 7 Professional.

Table 1 shows the file type and the performance of the two algorithms to encrypt ten different files of a thousand not shown in this article due to space shortage.

Table 1: Files, size and encryption time seconds

File Type	Size	Triple DES	Triple DES-96
JPEG Image (.jpg)	11.0KB	0.031	0-015
Sound Format (.mp3)	661 KB	1.903	1.092
power Point presentation (.pptx)	1.77 MB	5.257	2.995
Excel spreadsheet (.xisx)	3.09 MB	9.344	5.195
Access Data base (.accdb)	7.12 MB	21.013	12.090
WinRAR ZIP (.zip)	8.18 MB	25.1	14.134
Word 97-2003 Document(.doc)	22.0 MB	65.629	37.471
Adobe Acrobat Document (.pdf)	87.5 MB	257.884	146.843
Windows Media File (.wmv)	205 MB	606.014	347.884
Video MP4 (.mp4)	254 MB	756.562	428.236

Figure 6 shows a comparative graph of the execution measured in seconds of the two algorithms, and the results are considered efficient. It can be clearly seen, from table 1 that Triple DES-96 is up to 2.08 times faster than Triple DES.

The above different behavior is because; Triple DES-96 eliminates a permutation that takes place in each round. Combining Table E with Table P is achieved by running on a single time; however, the Triple DES cryptosystem applies two permutations. Furthermore, Triple DES-96 ciphers blocks of 96 bits instead of 64 bits as Triple DES does. This is why Triple DES-96 performs in almost half the time required by Triple DES.

5 Conclusions

Submitting information blocks of 96 bits achieved more information encrypted in a shorter period of time. Moving the E expansion table to output of the $SBoxes$ can combine it with the permutation P, and considering that the permutations E and P is performed 16 times by three cycles then, to perform this combination, 48 permutations are saved, as reflected in an increment of speed to encrypt information. By modifying the suite of encryption SSL/TLS Record Protocol to work with Triple DES-96, encryption and decryption of the information may be up to 2.08 times faster than when using Triple DES.

Acknowledgements The authors would like to thank the Universidad Autónoma del Estado de México; Instituto Politécnico Nacional (Secretaría Académica, COFAA, SIP and CIDETEC), the CONACyT, and SNI for their economical support to develop this work.

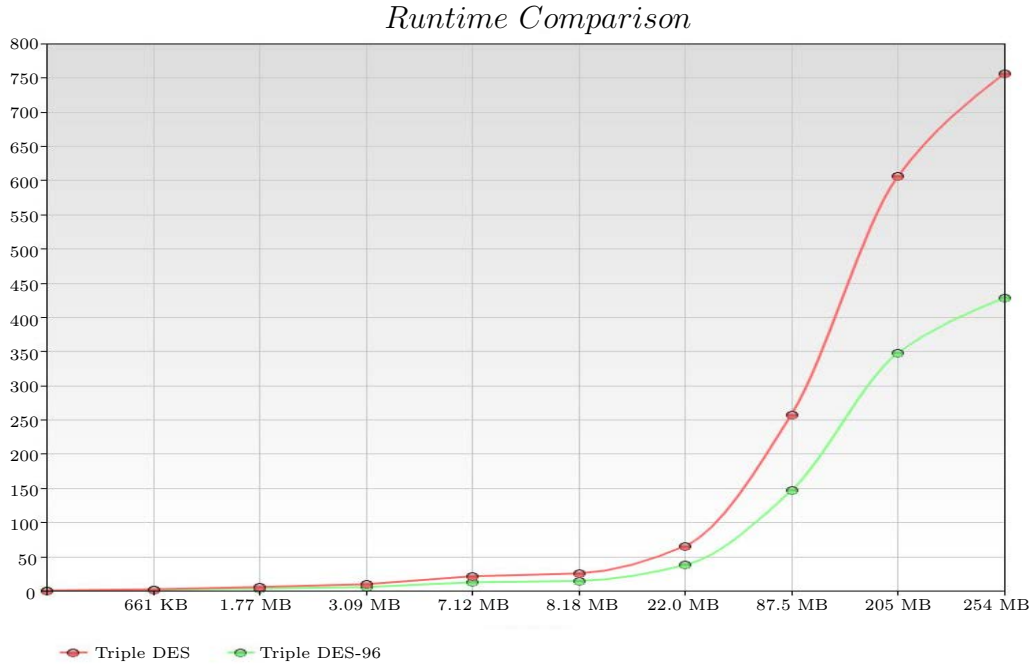

Figure 6: Graphical showing differences in rutine

References

[1] A. Baker, Transcendental Number Theory, Cambridge University Press, London, 1990, pp. 3-4.

[2] A. Freier, P. Karlton and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0", Netscape Communications, (2011).

[3] A. M. Muñoz, Intypedia Information Security Encyclopedia Lección 9. Introducción al protocolo SSL, España, 2011. Available at http://www.intypedia.com

[4] A. Maiorano, Criptografía técnicas de desarrollo para profesionales, Alfaomega, México, 2009, 221-222.

[5] B. Schneier, Applied Cryptography Protocols second edition: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., USA, 1995 pp. 265-284.

[6] D. O. Ramírez and C. C. Espinosa, El Cifrado Web (SSL/TLS), .Seguridad Cultura de Prevención Para TI Núm. 10, (2011).

[7] D. R. Stinson, Cryptography Theory and Practice Third Edition. Chapman & Hall/CRC, Canadá, 2006, pp. 95-102.

[8] Federal Information Processing Standards Publication 46-3, Data Encryption Standard (DES), U.S. Department of Commerce/National Institute of Standards and Technology (1999).

[9] J. Jaworski and P. J. Perrone, Edición Especial seguridad en Java, Prentice Hall, Madrid, 2001 pp. xviii.

[10] M. Hayoz and U. Ultes-Nitsche, Introducing SSL the Secure Sockets Layer Protocol, Switzerland, (2003).

[11] J. M. Dávila and E. R. Luna, Seguridad y comercio por internet, Conciencia Tecnológica (2000).

[12] Electronic Frontier Foundation, M. Loukides and J. Gilmore, Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design, O'Reilly & Associates, Inc., Sebastopol, CA, 1998.

[13] R. Duran, L. Hernández and J. Muñoz, Ataques a DES y Módulos de Factorización RSA, DIGITAL.CSIC, Madrid (2000).

[14] R. Flores, V. M. Silva, C. Rentería, DES BLOCK OF 96 BITS: AN APPLICATION TO IMAGE ENCRYPTION, International Journal of Research and Reviews in Applied Sciences, Vol. 14, Issue 1, (2013).

[15] T. Dierks and E. Rescorla, RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, Standard Tracks, Network Working Group, (2008).

[16] The Internet Engineering Task Force, 2014. Available at http://www.ietf.org/

[17] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, C. A. Jiménez Vázquez. Images encryption using AES and variable permutations. https://arxiv.org/submit/1070118/view

[18] V. M. Silva, R. Flores, C. Rentería and B. Luna, The Triple-Des-96 Cryptographic System, International Journal of Contemporary Mathematical Sciences HIKARI Ltd, (2013).

[19] W. Stallings, Cryptography and Network Security Principles and Practice Fifth Edition, Prentice Hall, Boston, 2010, pp. 489-506.

[20] W. Tuchman, Hellman presents no shortcut solutions to DES, IEEE Spectrum Vol. 16, No. 7, (1979) pp. 40-41.

Received: August 30, 2014