International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 1-4
©gopalax Journals, Singapore
available at : www.ijcns.com

PERFORMANCE ANALYSIS OF SYMMETRIC ENCRYPTION TECHNIQUES

E.Bharathi
Assistant professor
Department of Computer Applications,
Dr.SNS Rajalakshmi College of
Arts & Science, Coimbatore-641049

Dr.A.Marimuthu,
Associate Professor
Department of Computer Science,
Govt. Arts College(Autonomous),
Coimbatore – 641 018.

Dr.A.Kavitha,
Assistant Professor
Dept. of Computer Science,
Kongunadu Arts & Science
College,Coimbatore-641029

ABSTRACT

This paper deals with the present state in the field of symmetric key block ciphers, which are used for bulk data and link encryption. This paper focuses comparative analysis on different kinds of block cipher algorithms DES, RC6, BLOWFISH, UR5 algorithm, and study of literature survey on all the techniques. RC6 has 12 rounds, Blowfish & rounds UR5 with 8 rounds [10]. The study deals with the analysis of performance parameters used in the encryption process based on the security issues.

Keywords: Cryptography, Block Cipher, DES, RC6, Blowfish, UR5.

1. INTRODUCTION

The growth in internet and networking technology finds a way to a common culture of interchanging the data very fast. And it is more vulnerable of duplicating of data and re-distributed by hackers [1]. Therefore the sensitive information has to be protected while transmitting in a network. Many encryption techniques exist to avoid the information theft on transmission. Recently in wireless communication, encryption plays a vital role in securing the data.

Internet and networks applications are growing very fast, the increasing use of the secure transmission of data and information over the internet, so, the need of strong encryption algorithm increasing day by day. New methods of encryption techniques are discovered day to day. The security is based on cryptography; it is the art of message transfer with secure and immune to attacks by authenticating the sender to receiver. This paper holds some of the recent existing symmetric encryption techniques based on block cipher and their security issues. In cryptography, symmetric key encryption is common to ensure data confidentiality. Symmetric key uses same key for both encryption of plain text and decryption of cipher text. As illustrated in Fig (1).

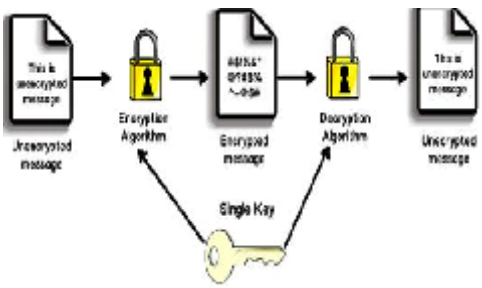

Figure. 1.1. Symmetric Key Encryption

2. BASIC TERMS IN CRYPTOGRAPHY

Plain Text: The original message that we wish to communicate with the others is defined as Plain Text. In cryptography the actual data that has to be send to the other is referred as Plain Text.

Cipher Text: The message which has been converted by the encryption algorithm is called cipher text. In Cryptography the original message is transformed into non readable message.

Encryption: A process of converting plain text into cipher text is called as Encryption. Cryptography uses the encryption algorithm and a key to send confidential data through an insecure channel.

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 1-4
©gopalax Journals, Singapore
available at : www.ijcns.com

Decryption: A reverse process of encryption is called decryption that is the process of converting cipher text into plain text. Decryption requires decryption algorithm and a key

3. GOALS OF CRYPTOGRAPHY

Cryptography provides a number of security goals to ensure the privacy of data, without any alteration of data. It is widely used today due to its security advantages [1]. Cryptography goals are listed below:

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures that either the sender, or the receiver of the message should be able to deny the transmission.

Access Control: Only the authorized parties are able to access the given information.

4. COMPARED ALGORITHMS

4.1 UR5

Fig (4.1) shows UR5 algorithm for Encryption and Decryption.UR5 is a block cipher symmetric encryption algorithm. This algorithm contains a series of transformation depending upon S-Box, XOR Gate and AND Gate. This algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits.UR5 contains 8 rounds for encryption and decryption process[11]. It is more efficient and useable for the Wireless Local Area Network because it avoids the using of the same key with packets within a message. The algorithm is simple and helps in avoiding the hackers from extracting the original data. The S-BOX generation is the main core of this algorithm. It contains eight columns and 256 rows; each element in it consists of 8-bits for the contents of S-boxes. It replaces the input by another code in each step of its eight rounds to produce output. Thus, in each encryption process, a new different key will be used for each round and it gives the impossibility to the hackers to decrypt the cipher text.

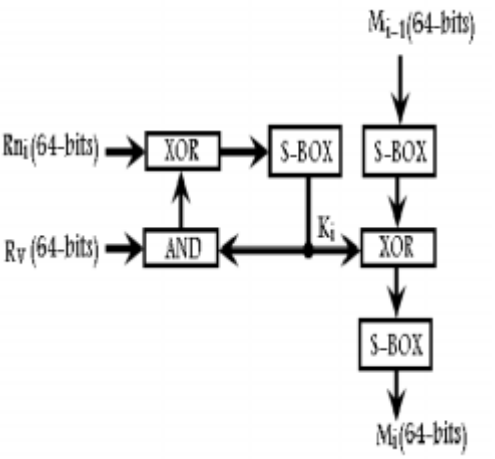

Figure. 4.1 UR5 Algorithm for Encryption or Decryption

4.2 Blowfish

Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms [4]. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key start from 32 bits to maximum 448 bits. Blowfish contains variants of 14 rounds or less. Blowfish is one of the fastest block ciphers which have developed to date. Slowness of encryption kept Blowfish from being used in some applications.

Blowfish have been created to allow anyone to use encryption free of patents and copyrights. Blowfish remains in the public domain to this day. No attack is known to be successful against it, though it suffers from the weak keys problem [7].

Fig (4.2) shows the action of Blowfish. Each line in it represents 32 bits. The algorithm has two sub keys arrays; 1) the 18-entry P-array2) Four 256-entry S-boxes. The S-boxes accepts 8-bit input and produce 32-bit output[8]. One entry of P-array is used for each round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 1-4
©gopalax Journals, Singapore
available at : www.ijcns.com

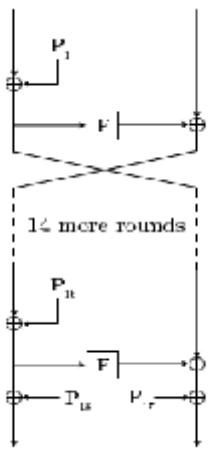

Figure. 4.2. Blowfish Encryption

4.3 RC6

Fig 4.3 shows RC6 Encryption and Decryption. RC6 is a symmetric block cipher algorithm [4]. It was designed by Ron Rivest, Ray Sidney, Matt Robshaw, and Yiqun Lisa Yin in the year 1998.It has a festal network structure with 20 rounds. RC6 is specified as RC6-w/r/b where the size of word is w bits, encryption must contain of a nonnegative number of rounds r and b which denotes the length of the encryption key in bytes. RC6 is similar to RC5 in structure, and use data-dependent rotations, and addition modulo 2w and XOR operations; and RC6 could be viewed as interweaving two parallel RC5 encryption processes [5]. RC6 use an extra multiplication operation which is not present in RC5 in order to make the rotation dependent on every bit in a word and not just the least significant few bits [6].

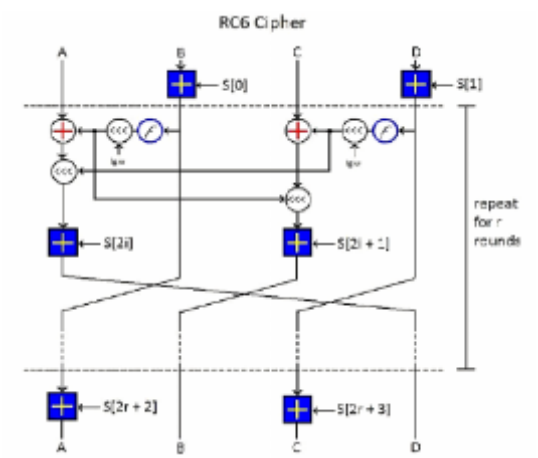

Figure.4.3 Encryption and Decryption

4.4 DES (Data Encryption Standard)

DES encryption process is illustrated in Fig 4.4. DES is developed in the early 1970s at IBM based on the earlier design by Horst Feistel, algorithm was submitted to the National Bureau of Standards (NBS)[9].It follows balanced Feistel network with 16 rounds.

DES is a symmetric algorithm; it uses one 64-bit key. Out of 64 bits, 56 bits are made independent key, which is used to determine the exact cryptography transformation, and 8 bits are used for error detection. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to that of encryption; (i.e.) the round keys used in encryption are applied in reverse order. The final output is a 64-bit block of cipher text [2].

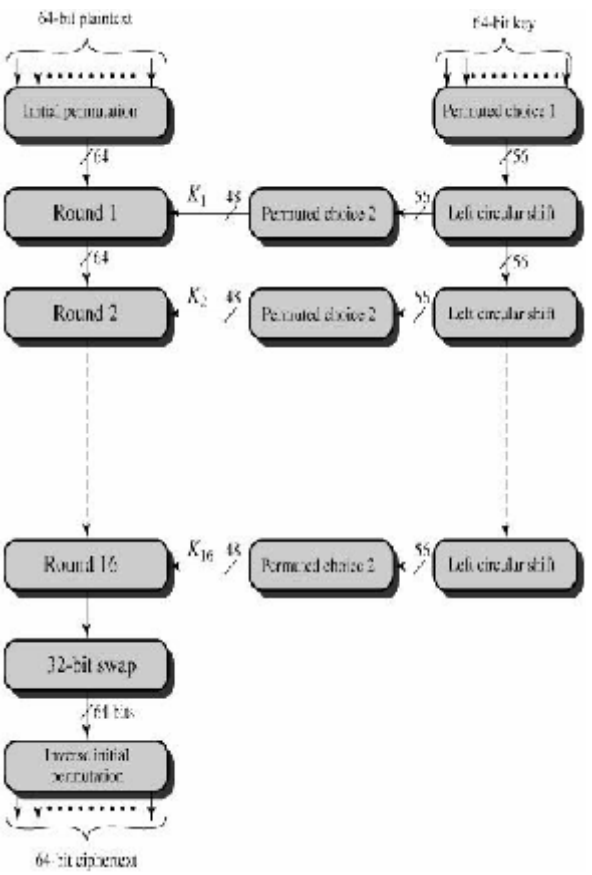

Figure. 4.4. DES Encryption Algorithm

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 1-4
©gopalax Journals, Singapore
available at : www.ijcns.com

5. PARAMETRIC COMPARISON

Table 1 summarizes the comparison of UR5, Blowfish, RC6 and DES for different design parameters such as word size, block size, number of rounds and secret key size.

Table 1: Parametric Comparison

Parameters	UR5	Blowfish	RC6	DES
b (key length in bytes)	64 bits	16, 24 or 32	0 - 255 (standard 16)	8
r (no of rounds)	8	16	0 - 255 (standard 20) [10]	16
No of round keys	R_v & R_{ni}	r+2	r + 4	r
Block size in words	5w	2w	4w	2w
w (word size in bits)	64	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)
Block size in bits	128,192 ,256 (Standard 128)	32, 64, 128 (standard 64)	64, 128, 256 (standard 128)	32, 64, 128 (standard 64)
Used Function	S-Box	S-Box	F(x) = x(2x+1) mod 2w	IP, IP-1, E, P, S-Box, PC-1, PC-2
Used Operation	And gate, Xor gate	+, ⊕, <<<, >>>	+, -, ⊕, *, <<<, >>>	⊕, <<<, >>>
Attacks	Not Yet	Not Yet	Statistical	Brute Fore

The security of any algorithm is highly based on the length of key being used. In the above table it is clear that the key size of UR5 algorithm is high. Hence it can be said that security of UR5 is better than the other algorithms.

6. CONCLUSION

This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, RC6, Blowfish and UR5. The security aspect of Symmetric key encryption is superior. The comparison table of popular encryption algorithms clearly shows the supremacy of UR5 over DES, RC6 and Blowfish on the basis of block size and security. The F function of UR5 algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the UR5 algorithm runs faster than other symmetric key encryption algorithms in some metrics.

REFERENCE

1. W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.
2. National Bureau of Standards, "Data Encryption Standard," FIPS Publication 46, 1977.
3. Ronald L. Rivest, M.J.B. Robshaw, R. Sidney and Y.L.Yin, The RC6 TM Block Cipher , M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, Version 1.1 - August 20, 1998. Available on the site: http://people.csail.mit.edu/rivest/Rc6.pdf
4. "RC6® Block Cipher" http://www.rsa.com/rsalabs/node.asp?id=2512
5. "RC6"http://en.wikipedia.org/wiki/Rc6
6. Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, "An improved RC6 algorithm with the same structure of encryption and decryption" ISBN 978-89-5519-139-4, Volume : 02, ICACT 2009, IEEE
7. B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", [online] Available at: http://www.schneier.com/paper-blowfish-fse.html
8. "Blowfish", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Blowfish_(cipher) .
9. "Data Encryption Standard", "wikipedia.org", [online] Available at: http://en.wikipedia.org/wiki/Data_Encryption_Standard
10. Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms *Volume 42– No.16, March 2012*
11. G.Ramesh and R.Umarani ' A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms http://research.ijcaonline.org/volume46/number13/pxc3879401.pdf.