 ISSN: 2321-8169
4301 - 4306

Critical Analysis of Various Symmetric Key Cryptographic Algorithms

Preksha Nema
Dept. of Computer Engineering and Applications
National Institute of Technical Teachers' Training and Research
Bhopal (M.P), India
preksha.nema@gmail.com

M.A.Rizvi
Dept. of Computer Engineering and Applications
National Institute of Technical Teachers' Training and Research
Bhopal (M.P), India
marizvi@nitttrbpl.ac.in

Abstract—Current era is digital and has elite advancement in technology, almost in every field things are becoming technology friendly. It is the need to provide security to sensitive information in this fast growing technical world. Cryptography is one of the very popular fields of network security that deals with conversion of sensitive data into one which could not be understood by anyone without the secret key. Many researchers has worked in the area of cryptography and developed many algorithms in different period and providing security to the travelling data. It is need to know the strengths and weakness of each algorithm before using and suggesting to anybody to use one. After critically analyzing existing standard cryptographic algorithms on parameters like throughput, power consumption and memory usage on DES, TDES, AES, Blowfish, Twofish, Threefish, RC2, RC4, RC5 and RC6, it has been concluded that which algorithm will suit in which situation.

Keywords-Cryptography; Encryption; Decryption; symmetric key encryption; asymmetric key encryption

*****

I. INTRODUCTION

Network security is one of the field of computer technology having its vast dimensions that covers computer (Information) security, network security as well as the internet security. Security is one of the most significant issues to be kept in mind while doing any work that is dependent on computer network. Today in this mobile era of bits and bytes everyone is dependent on technology that uses the computer network and internet.

- Computer Security - generic name for the collection of tools designed to protect data from hackers.
- Network Security - measures to protect data during transmission.
- Internet Security - measures to protect data during Internet access. [1]

This Security is the foremost requirement to be fulfilled. As the growth of security measures increases, the attacks on security are also growing proportionally. Intruders and attackers are always finding out opportunity to hack data that is being transmitted. In order to win this war for preserving security, there is the desperate need of some very strong measures against these malicious intruders. Cryptography is one of the most common and fruitful measure against them. In this paper an analysis is done on various cryptographic algorithms with some parameters.

Cryptography means secret writing (crypto- means secret and graphy means- writing) as illustrated in figure1. It is having two main processes that are encryption at sender side and decryption at receiver side. Modern cryptography uses mathematical techniques to provide security services and relies upon two basic components [2]:

- An Algorithm (or Cryptographic methodology)
- A Cryptographic Key which determines the specifics of algorithm operation.

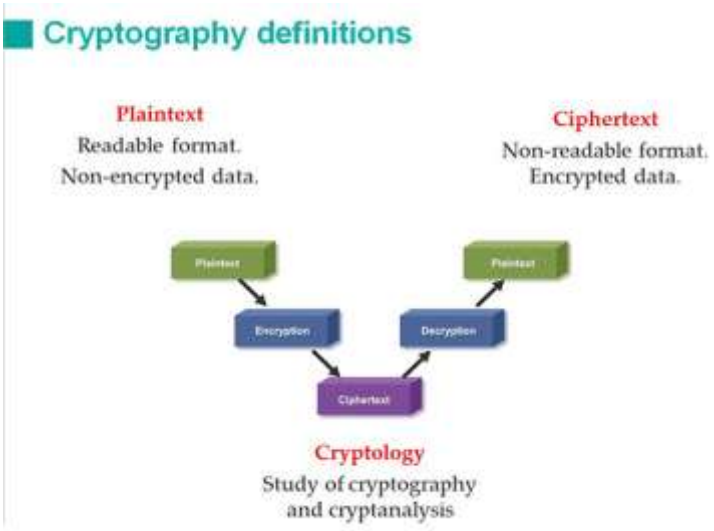

Figure 1: Concept of cryptography

A. BASIC TERMINOLOGY

- Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form
- Plaintext: The original intelligible message
- Cipher text: The transformed message

 ISSN: 2321-8169
4301 - 4306

- Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- Key: Some critical information used by the cipher, known only to the sender& receiver
- Encipher: (encode) The process of converting plaintext to cipher text using a cipher and a key
- Decipher: (decode) the process of converting cipher text back into plaintext using a cipher and a key

Cryptography is used to provide following security objectives of confidentiality, Authentication, integrity, Non- repudiation, Access control:

- 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 neither the sender, nor the receiver of message should be able to deny the transmission.
- Access control: Only the authorized parties are able to access the given information.

Cryptographic methods are categorized according to the following three ways [3]:

- Type of operations used for transforming plaintext to cipher text: All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plaintext is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.
- The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.
- The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

Symmetric Key cryptography: In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. A symmetric-key (Private-key) cipher involves a sender (A) and a receiver (B) choosing a key k which eventually gives rise to an encryption rule ek and a decryption rule dk.

Examples: AES Algorithm, DES algorithm, Blowfish algorithm, Triple DES algorithm.

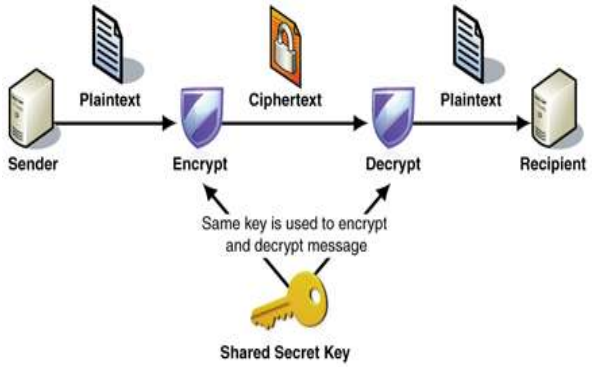

Figure2: symmetric key cryptography

Asymmetric Key Cryptography: Asymmetric key encryption is the technique in which the keys are different for the encryption and the decryption process. One of these keys is published or public and the other is kept private. They are also known as the public key encryption. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted. Examples are RSA algorithm, differ-Hellman.

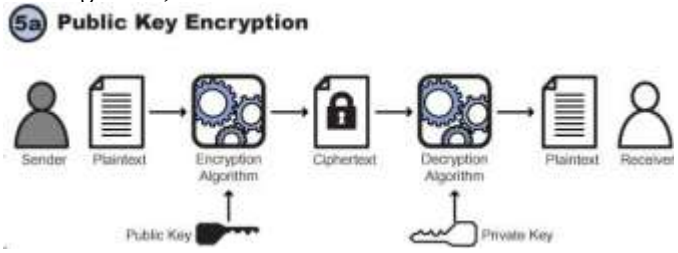

Figure3: Asymmetric key cryptography

Some critical parameters on which the different algorithms are being analyzed are [4];

- Architecture

Defines the structure and operations that an algorithm can perform, its characteristics and how they are implemented. It also determines that the algorithm is symmetric or asymmetric that is whether it makes use of secret key or public key for encryption and decryption.

- Security

An affirmative measure of the system strength in resisting an attack is a desirable element of any encryption algorithm possesses the property of in distinguishability (built by combining substitution with transposition repeatedly). Security of an encryption algorithm depends on the key size used to execute the encryption: generally, greater the keys size stronger the encryption. Length of key is measured in bits.

- Scalability

It is one of the major element on which encryption algorithms can be analyzed. Scalability depends on certain parameters such as Memory Usage, Encryption rate, Software hardware performance; Computational efficiency.

- Limitations (Known Attacks)

Defines how fine the algorithm works by make use of the computer resources available to it. Further how often is vulnerable to different types of attacks.

 ISSN: 2321-8169
4301 - 4306

II. DISCRIPTION

A. Data Encryption Standard

DES is a block cipher that uses shared secret key for encryption and decryption. DES algorithm as described by Davis R. takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. DES also uses a key of 56 bits to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt the message. There are 16 identical stages of processing, termed rounds. There is also an initial and final permutation, termed IP and FP, which are inverses (IP "undoes" the action of FP, and vice versa). The Broad level steps in DES are as follows [5]:

1. In the first step, the 64-bit plain text message is handed over to an Initial permutation (IP) function.
2. The initial permutation is performed on plain text.
3. The IP produces two halves of the permuted message; Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now, each of LPT and RPT go through 16 rounds of encryption process.
5. In the end, LPT and RPT are rejoined and a final permutation (FP) is performed on the combined block.
6. The result of this process produces 64-bit cipher text. Rounds: Each of the 16 rounds, in turn, consists of the broad level steps and shown in Figure 3.1.

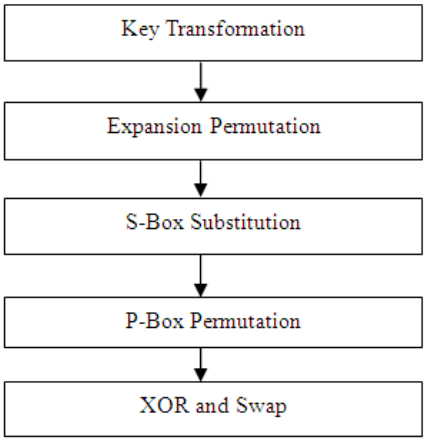

Figure 4: Details of One Round in DES

B. Triple DES

It is an enhancement of DES. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt- Encrypt (EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message, t. C(t) = Ek1(Dk2(Ek3(t))) ,Where C(t) is cipher text produced from plain text t, Ek1 is the encryption method using key k1, Dk2 is the decryption method using key k2 ,Ek3 is the encryption method using key k3. Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.C(t) = Ek1(Dk2(Ek3(t))).

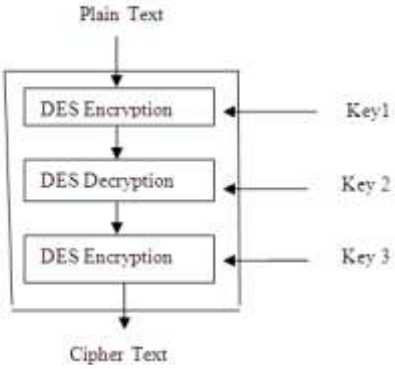

Figure 5: Encryption in 3DES

TDES algorithm with three keys requires 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combination so TDES is a strongest encryption algorithm. The disadvantage of this algorithm it is too time consuming. [5]

C. Advanced Encryption Standard

The AES cipher is almost identical to the block cipher Rijndael cipher. AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128- bit key is 10. Unlike its predecessor DES, AES does not use a Feistel network. Feistel networks do not encrypt an entire block per iteration, on the other hand, AES encrypts all 128 bits in one iteration. This is one reason why it has a comparably small number of rounds. [5]

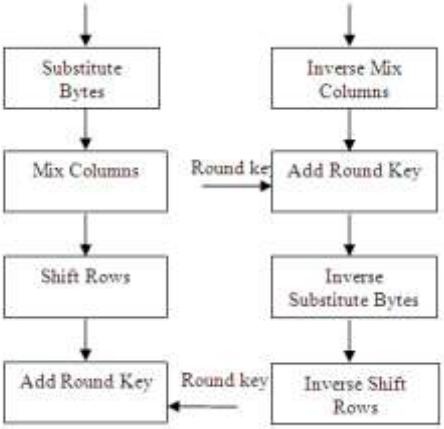

Figure 6: One Round of encryption and Decryption in AES

Encryption Round Decryption Round Each processing round involves four steps:-

- Substitute byte: a non-linear substitution step where each byte is replaced with another according to a lookup table.
- Shift rows: a transposition step where each row of the state is shifted cyclically a certain number of steps.

- Mixcoloumn: a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add round key: each byte of the state is combined with the round key using bitwise XOR. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

D. Blowfish

Blowfish is one of the most common public domain encryption algorithms. It contains two parts Subkey Generation: This process converts the key upto 448 bits long to subkeys to totaling 4168 bits and Data Encryption: This process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation and key- and data dependent substitution. Blowfish suits the applications where the key remain constant for a long time (e.g. communication link encryption) but not where the key changes frequently (e.g. packet switching) [5].

E. Two fish

It is a symmetric key block cipher and was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Two fish is related to the earlier block cipher Blowfish. Two fish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes).

The Two fish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Two fish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the Open PGP standard (RFC 4880). However, Two fish has seen less widespread usage than Blowfish, which has been available longer [6].

F. Three fish

Three fish is a symmetric-key tweak able block cipher designed as part of the Skein hash function, an entry in the NIST hash function competition. Three fish uses no S-boxes or other table lookups in order to avoid cache timing attacks;[1] its nonlinearity comes from alternating additions with exclusive ORs. For the 32-round version, the time complexity is 2^{226} and the memory complexity is 2^{12} ; for the 33-round version, the time complexity is $2^{352.17}$ with a negligible memory usage. The attacks also work against the tweaked version of Three fish: for the 32-round version, the time complexity is 2^{222} and the memory complexity is 2^{12} ; for the 33-round version, the time complexity is $2^{355.5}$ with a negligible memory usage[6].

G. RC2

RC2 (also known as ARC2) is a symmetric block-key where "RC" stands for "Ron's Code" or "Rivest Cipher". It was considered as a proposal for the DES replacement. If the key encryption has been performed beforehand, then this algorithm runs twice as fast as DES on an IBM AT. The algorithm itself involves 3 further sub algorithms viz. Key Expansion, Encryption, and Decryption. This was designed as a proposal to replace the existing DES Algorithm.Its 18 rounds are arranged as a source-heavy Feistel network, with 16 rounds of one type (*MIXING*) punctuated by two rounds of another type (*MASHING*). A MIXING round consists of four applications of the MIX transformation.RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [7][14].

H. RC4

RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The data stream is simply XORed with the series of generated keys. The key stream does not depend on plaintext used at all. A variable length key from 1 to 256 bit is used to initialize a 256-bit state table. Vernam stream cipher is the most widely used stream cipher based on a variable key-size. It is popular due to its simplicity. It is often used in file encryption products and secure communications, such as within SSL. The WEP (Wireless Equivalent Privacy) protocol also used the RC4 algorithm for confidentiality. It was also used by many other email encryption products. The cipher can be expected to run very quickly in software. It was considered secure until it was vulnerable to the BEAST attack [14].

I. RC5

RC5 is a symmetric-key block cipher notable for its simplicity. The Advanced Encryption Standard (AES) candidate RC6 was based on RC5. Unlike many schemes, RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choices of parameters were a block size of 64 bits, a 128-bit key and 12 rounds.

A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive. RC5 also consists of a number of modular additions and eXclusive OR (XOR)s. The general structure of the algorithm is a Feistel-like network.The encryption and decryption routines can be specified in a few lines of code. The key schedule, however, is more complex, expanding the key using an essentially one-way function with the binary expansions of e. The tantalizing simplicity of the algorithm together with the novelty of the data-dependent rotations has made RC5 an attractive object of study for cryptanalysts. The RC5 is basically denoted as RC5-w/r/b where w=word size in bits, r=number of rounds, b=number of 8-bit byte in the key [7].

J. RC6

RC6 (Rivest Cipher *6*) is a symmetric key block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and also was submitted to the NESSIE and CRYPTREC projects. It is a proprietary algorithm, patented by RSA Security. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, however, RC6 does use an extra multiplication operation 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 [7].

We have analyzed various cryptographic algorithms based on some significant and remarkable parameters. Appendix I contains the Table1 that shows the detailed analysis of immense research work which has been already done by researchers. After the analysis it is being summarized that each algorithms have their own merits and demerits and this is totally application dependent that which parameter is the basic requirement of the particular application or a user. So based on the need of application the particular algorithm can be chosen. According to our perspective throughput and the strength of algorithms are the two major parameters and Blowfish algorithm performance is better. So among these entire cryptographic algorithm Blowfish is comparatively higher efficient with respect to others.

III. CONCLUSION

In this paper critical analysis of various cryptographic algorithms is done based on some important parameters such as throughput, scalability, security, memory usage, power consumption, speed and flexibility. The major strengths and limitations of the mentioned algorithms make them transparent for various applications. During this analysis it was observed that Blowfish was the best among all in terms of Security, Flexibility, Memory usage, and Encryption performance. Although the other algorithms were also competent but most of them have a tradeoff between memory usage and encryption performance with few algorithms been compromised. It can be concluded that one can choose cryptographic algorithm based on the type of application and most important feature concern.

REFERENCES

[1] W. Stallings, "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007
[2] csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf
[3] Omkar Guru, Sanjay Majumdar, Krithika K, "Implementaion of cryptographic algorithms and protocals".
[4] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid "Symmetric Algorithm Survey: A Comparative Analysis" International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.
[5] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Techniques" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014 ISSN 2278-6856.
[6] G. Muthukumar, Dr. E. George Dharma Prakash Raj "A Comparative Analysis on Symmetric Key Encryption Algorithms" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.
[7] T.Gunasundari1, Dr. K.Elangovan "A Comparative Survey on Symmetric Key Encryption Algorithms" International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 2, February- 2014, pg. 78-83 ISSN: 2321-8363.
[8] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS" International Journal of Advanced Engineering Technology E-ISSN 0976-3945
[9] Narender Tyagi, Anita Ganpati "Comparative Analysis of Symmetric Key Encryption Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 8, August 2014 ISSN: 2277 128X.
[10] Nivedita Bisht, Sapna Singh "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms" International Journal of Innovative Research in Science Engineering and Technology Vol. 4, Issue 3, March 2015.
[11] Ms.K.Durgadevi, Ms. Selvanathiya, Mr.M.Sivasubramanian "IMPLEMENTATION OF SECURE MASTER USING MODIFIED TWOFISH ALGORITHM IN FPGA DEVICES" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 1, Issue 3, pp.507-512507.
[12] Milind Mathur, Ayush Kesarwani "COMPARISON BETWEEN DES, 3DES, RC2, RC6, BLOWFISH AND AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.
[13] D. Naga Swetha "Histogram based comparison on Symmetric Encryption Algorithms of Information Security" IJCSET August 2012 Vol 2, Issue 8, 1377-1382 ISSN:2231-0711.
[14] Sheetal Charbathia and Sandeep Sharma "A Comparative Study of Rivest Cipher Algorithms" International Journal of Information & Computation Technology ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1831-1838.
[15] Diaa Salama Abd Elminaam "Evaluating The Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.
[16] G.Ramesh "A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms" International Journal of Computer Applications (0975 – 8887) Volume 46– No.13, May 2012.
[17] MD Asif Mushtaque "Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity" International Journal of Engineering Research & Technology (IJERT) IJERTIJERT ISSN: 2278-0181 Vol. 3 Issue 4, April – 2014.
[18] Mohammad Rafeek Khan, Md Imran Alam "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 10, October 2013 ISSN: 2277 128X.
[19] Lalit Singh, Dr. R.K. Bharti "Comparative Performance Analysis of Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 11, November 2013 ISSN: 2277 128X.
[20] http://www.nada.kth.se/kurser/kth/2D1441/semteo03/lecturenotes/rapport_SS-OW_semteo.pdf
[21] www.academia.edu/9128513/Computer_Network_Attacks_A_Study
[22] www.brighthub.com › ... › Enterprise Security › Network Security.
[23] www.nada.kth.se/kurser/kth/2D1441/.../rapport_SS-OW_semteo.ps
[24] Rajani Devi.T, "Importance of Cryptography in Network Security" International Conference on Communication Systems and Network Technologies, 2013
[25] Soumyabrata Dev, (IEEE, Student Member); Ziaul Haque Choudhury , "A randomized cryptographic algorithm and its simulation in C and MATLAB with its hardware implementation in Verilog HDL"
[26] Dr. V.U.K.Sastry, K. Shirisha, "A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix()" at Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 9 ,April 2013
[27] Nehal Kandele, Shrikant Tiwari, "New cryptography method using dynamic base tansformation:DBTC symmeric key algoithm" at International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 4, July 2012
[28] http://www.cs.iit.edu/cs549/lectures/CNS-1.pdf,CS595
[29] E. Cole, R. Krutz and J. W. Conley, Network Security Bible,Wiley Publishing Inc, 2005.
[30] Sidhpurwalahuzaifa. A Brief History of Cryptography. [Online].Available:https://securityblog.redhat.com/2013/08 /14/a-briefhistory-of-cryptography/
[31] Manas Paul, and Jyotsna Kumar Mandal, "A Universal Bit Level Block Encoding Technique Using Session Based Symmetric Key Cryptography to Enhance the Information Security", International Journal of Advanced Information Technology, Vol. 2, No.2, DOI 10.5121/ijait.2012.2203, pp. 29-40, 2012

APPENDIX I

Table1: COMPARISON BETWEEN VARIOUS ALGORITHMS BASED ON SOME OF THE PARAMETERS WITH TABULAR ANALYSIS

S.no.	Features	DES	TDES	AES	BLOWFISH	TWO FISH	THREE FISH	RC2	RC4	RC5	RC6
1.	Developed by and year:	IBM 1975	IBM 1978	Joan Daeman, Vincet Rijmen 1998	Bruce Schneier 1993	Bruce Schneier 1998	Bruce Schneier, Stefan lucks 2008	Ron Rivest 1994	Ron Rivest (RSA Security) 1994	Ron Rivest 1994	Yiqun Lisa Yin 1998
2.	Algorithm Type	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric	Symmetric
3.	Algorithm structure	Feistel Network	Feistel Network	Substitution, Permutation Network	Feistel Network	Feistel N/w	S-box	Feistel N/w	Feistel N/w	Feistel N/w	Feistel N/w
4.	Block size(in bits)	64	64	128	64	128	256, 512, or 1024	64	2,064 (1,684 effective)	32, 64 or 128	128
5.	Rounds	16	48	10,12,14	16	16	72	16	256	1-255	20
6.	Key length(in bits)	56	112, 168	128, 192 or 256	32 to 448	128, 192, or 256	256, 512, or 1024	8–1024	40– 2,048	0 to 2040	128, 192, or 256
7.	Power consumption	Medium	High	High	Lowest	Low	High	High	High	High	medium
8.	Encryption throughput	Medium	Low	High	Very High	Medium	Medium	Medium	High	High	High
9.	Decryption throughput	Medium	Low	High	Very High	Medium	Medium	Medium	High	High	High
10.	Algorithm Strength	Secure	Secure	Secure	Highly Secure	vulnerable	Highly Secure	vulnerable	vulnerable	Conditionally secure	Considered vulnerable
11.	Speed	Fast	Moderate	Fast	Very fast	Less than AES	Moderate	Very Fast	Fast	Fast	Faster than RC2
12.	Memory usage	High	Very High	Medium	Very low	low	Very low	Low	Low	Low	Low
13.	Attacks	Brute force	Brute force	Brute force	Dictionary	Differential	Rotational with Rebound	brute force	brute force	Differential	Brute force
14.	Implementation	Complex	Complex	Simple	Simple	Simple	Simple	Simple	Simple	Complex	Complex
15.	Flexible	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes