Indian Journal of Research Communication Engineering (IJRCE)
Vol.3.No.1 2015 pp 17-27
available at: www.goniv.com
Paper Received :20-03-2015
Paper Accepted:14-04-2015
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

A SURVEY ON VARIUOS ENCRYPTION AND DECRYPTION ALGORITHMS

T. Balasubramanian
Assistant Professor
Sri Vidhya Mandir Arts & Science College
Katteri, Uthangakari -635 307.

Abstract

Computer networks were primarily used by university researchers for studying e-mail, and by corporate employees for sharing printers. Security was not an important issue at that time. But now as billions of ordinary citizens are using networks for banking, shopping, Air Ticketing, Online Examinations and filling their income tax returns. Network security has become an important issue and potentially massive problem in data communication. Most security problems are intentionally caused by malicious people trying to gain some benefit or harm someone. This paper provides a review and survey in between some symmetric and asymmetric techniques. The factors are achieving an effectiveness, flexibility and security, which is a face of researchers. As a result, the better solution to the symmetric key encryption and the asymmetric key encryption is provided.

Keywords- Encryption, Decryption,Cryptography, Data Encryption standard(DES), Asymmetric Encryption standard(AES), Symmetric Encryption, Asymmetric Encryption

---

I. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to seeming nonsense. The originator of an encrypted message shared the decoding technique needed to recuperate the original information only with intended recipients, thereby precluding undesirable persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. Cryptography includes the following process:

A. Encryption and Decryption

It is the process of converting ordinary information (called plaintext) into unintelligible text (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher is a pair of algorithms that create the encryption and the reversing

decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

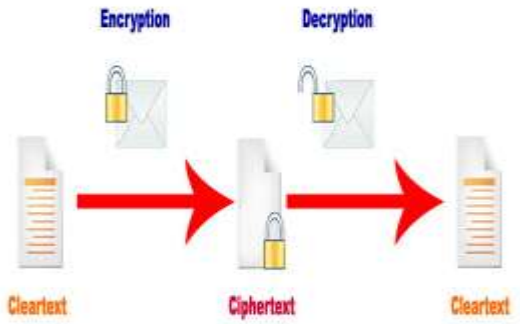

Figure 1.1 Process of Encryption and Decryption

II. Background

Cryptography is the art and science of keeping messages secure. The required basic definitions and concepts [23] in Cryptography are reviewed here.

- Plaintext: An original message is called Plain text or cleartext.
- Encryption: Process of modifying a message to hide its substance.
- Ciphertext: An encrypted message is Ciphertext.
- Decryption: Process of turning Ciphertext back into Plaintext is called Decryption.
- Cryptanalysis: Cryptanalysis is the science of recovering the plaintext of a message without access to the key.

III. Overview of Existing Algorithms

A. Data Encryption Standard (DES)

DES was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960‟s which resulted in a cipher known as LUCIFER. The altered version of LUCIFER was put forward as a proposal for the new national encryption standard requested by the National Bureau of Standards (NBS). It was finally adopted in 1977 as the Data Encryption Standard –DES. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70‟s. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded [19][24]. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and R i which are then passed into 16 rounds (the subscript i in Li and Ri indicates the current round). Each of the rounds are identical and the effects of increasing their number are twofold - the algorithms, security is increased and its temporal efficiency decreased. Clearly, these are two conflicting outcomes and a compromise must be made. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key. At the end of the 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output. This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bits ciphertext [21] [23].

B. Triple Data Encryption Standard (3DES)

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA)

block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryptor, we simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The Triple DES DLL then breaks the user provided key into three subkeys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key [22]. C. Advanced Encryption Standard (AES) AES emerged as a powerful replacement of DES during a competition held by National Institute of Standard and Technology (NIST). The competition was organized to develop a substitute of existing DES. Rijndael: an algorithm designed by Daemen and Rijmen was judged the best and announced to be new AES. NIST choose Rijndael, due to its simplicity and high performance. It is fast, compact, and has a very simple mathematical structure [4].AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds [23]. The main loop of AES performs the following functions: 1. SubBytes () 2. ShiftRows () 3. MixColumns () 4. AddRoundKey (). The first three functions of an AES round are designed to thwart cryptanalysis via the Methods of "confusion" and "diffusion." The fourth function actually encrypts the data. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially MixColumns () and Shiftrows (). AES can be attacked using the Timing analysis Attack. This occurs when Malice (the malicious Alice) runs the Sub-Bytes method on different data and observes the time it takes for each execution.

C. AES (Advanced Encryption Standard)

AES is also known as the Rijndael's algorithm, is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It encrypts data blocks of 128 bits using symmetric keys. It has a variable key length of 128, 192 or 256 bits : by default 256 is used. AES encrypts 128 bit data block into 10, 12 and 14 rounds according to the key size. AES can be implemented on various platforms such as small device encryption of AES is fast and flexible. AES has been tested for many security applications. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies.

D. Blowfish

It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure

cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak key problem.

E. IDEA(International Data Encryption Algorithm)

IDEA is a block cipher algorithm and it operates on 64-bit plaintext blocks. The key size is 128 bits long. The design of algorithms is one of mixing operations from different algebraic groups. Three algebraic groups are mixed, and they are easily implemented in both hardware and software: XOR, Addition modulo 216 , Multiplication modulo 216 + 1. All these operations operate on 16-bit sub-blocks. This algorithm is efficient on 16-bit processors. IDEA is symmetric key algorithm based on the concept of Substitution-Permutation Structure, is a block cipher that uses a 64 bit plain text with 8 rounds and a Key Length of 128-bit permuted into 52 sub-keys each of 128- bits. It does not contain S-boxes and same algorithm is used in reversed for decryption .

F. RC4

RC4 is a stream cipher symmetric key algorithm. as the data stream is simply XOR with generated key sequence. It uses a variable length key 256 bits to initialize a 256-bit state table. A state table is used for generation of pseudo-random bits which is XOR with the plaintext to generate the cipher text.

G. RC6

RC6 is a derivative of RC5. RC6 is designed by Matt Robshaw, Ron Rivest Ray Sidney and is a symmetric key algorithm that is used to congregate the requirements of AES contest . RC6 was also presented to the CRYPTREC and NESSIE projects. It is patented by RSA Security . RC6 offers good performance in terms of security and compatibility. RC6 is a Feistel Structured private key algorithm that makes use a 128 bit plain text with 20 rounds and a variable Key Length of 128, 192, and 256 bit. As RC6 works on the principle of RC that can sustain an extensive range of key sizes, word-lengths and number of rounds, RC6 does not contain S- boxes and same algorithm is used in reversed for decryption.

H. Serpent

Serpent is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, is a symmetric key block cipher, designed by Eli Biham, Ross Anderson, and Lars Knudsen. Serpent is a symmetric key algorithm that is based on substitution-permutation network Structure. It consists of a 128 bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It also contains 8 S- boxes and same algorithm is used in reversed for decryption. Security presented by Serpent was based on more conventional approaches than the other AES finalists. The Serpent is open in the public sphere and not yet patented.

I. Twofish

Twofish is also a symmetric key algorithm based on the Feistel Structure and was designed by Bruce Schneier along with Doug Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall,. The AES is a block cipher that uses a 128 bit plain text with 16 rounds and a variable Key Length of 128, 192, 256 bit. It makes use of 4 S-boxes (depending on Key) and same algorithm is used in reversed for decryption. The inventors extends the Blowfish team to enhance the earlier block cipher Blowfish to its modified version named Twofish to met the standards of AES for algorithm designing. It was one of

the finalists of the AES, but was not selected for standardization. The Twofish is an open to public sphere and not yet patented.

J. TEA

TEA is also a Feistel Structured symmetric key algorithm. TEA is a block cipher that uses a 64 bit plain text with 64 rounds and a Key Length of 128-bit with variable rounds having 32 cycles. It does not contain S- boxes and same algorithm is used in reversed for decryption. TEA is designed to maximize speed and minimize memory footprint. Cryptographers have discovered three related-key attacks on TEA. Each TEA key can be found to have three equal keys, thus it can be used as a hash function. David Wheeler and Roger Needham have proposed extensions of TEA that counter the above attacks.

K. CAST

CAST is symmetric key algorithm based on the backbone concept of Feistel Structure. It is designed by Stafford Taveres and Carlisle Adams, is considered to be a solid algorithm. The CAST is a block cipher that uses a 64 bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S- boxes and same algorithm is used in reversed for decryption. Bruce Schneier , John Kelsey, and David Wagner have discovered a related-key attack on the 64 bit of CAST that requires 217 chosen plaintexts, one related query, and 248offline computations. CAST is patented, which was generously released it for free use.

N. Diffie-Hellman

This algorithm was introduced in 1976 by Diffie-Hellman. In it, each party generates a key pair and distributes the public key. After obtaining an authentic copy of public keys, then shared secret can be used as the key for a symmetric cipher .The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure communication channel . One way authentication is free with this type of algorithm. The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack.

O. MD5

MD5's full form is message-digest algorithm. MD5 is derived from MD4 & was designed by Ron Rivest in 1991 . MD5 is widely used hash function producing a 128-bit hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

IV. LITERATURE REVIEW

Network security and cryptography challenges and issues are discussed by various researchers. In this section various literature reviews of different researchers are presented.

Singh et al. [16] made the comparison between DES, 3DES, AES and Blowfish symmetric algorithms. The comparison had been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithms encryption/decryption speed. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time.

Cornwell [5] discussed the design of Bruce Schneier‟s Blowfish encryption algorithm along with a performance analysis and

possible attacks. It was concluded about the effectiveness of Blowfish with the other well known algorithms DES, 3DES, and AES. It was concluded that Blowfish is able to provide long term data security without any known backdoor vulnerability or ability to reduce the key size. For the future scope Blowfish was considered safe and effective design although future reevaluations will be needed.

Tamimi [18] compared DES, 3DES, AES and Blowfish symmetric algorithms. The performance of these algorithms under different settings, and different data loads were considered. This study used two modes of operation i.e. ECB and CBC for calculating execution time of each algorithm. This study used C# programming language for simulation. It was concluded that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results as compared to other algorithms, because it required more processing time. CBC mode had added extra time, but it was relatively negligible.

Nadeem [11] discussed the popular secret key algorithms DES, 3DES, AES (Rijndael), Blowfish and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in Java programming language, and were tested on different hardware platforms, to present the comparison. The two different machines were: P-II 266 MHz and P-IV 2.4 GHz. It was concluded that Blowfish had an advantage over other algorithms. Also it showed that AES has better performance than DES and 3DES. Also it was concluded that 3DES needs 3 times than DES to process the same amount of data.

Dhawan [6] compared the performance of the different encryption algorithms by conducting experiments inside .NET framework. The comparison was performed on the following algorithms: DES, 3DES, RC2, and AES (Rijndael). It was concluded that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

Singh et al. [15] performed a comparison between the most common four encryption algorithms namely; AES, DES, 3DES and Blowfish in terms of security and power consumption. Experiment results of comparison were carried out over different data types like text, image, audio and video. The simulation results showed that AES has a better performance than other common algorithms. AES is supposed to be better algorithm which was compared to original Blowfish Algorithm. But adding additional key and replacing the old XOR by new operation „#“ as a purposed by this study to give more robustness to Blowfish Algorithm and make it stronger against any type of intrusion. This advance Blowfish Algorithm is more efficient in energy consumption and security to reduce the consumption of battery power device.

Agrawal et al. [2] made a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption. It was concluded that the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data. Also the Blowfish algorithm runs faster than other popular symmetric key encryption algorithms.

Seth et al. [14] made a comparative analysis of three algorithms, DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool was used for conducting experiments. It was concluded that RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Based on the text files used and the experimental result it was concluded that DES consume least encryption time and AES has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

Mandal et al. [9] made the comparison between four most commonly used Symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of parameters: round block size, key size, encryption/decryption time, and CPU process time in the form of throughput and power consumption. It was concluded that blowfish is better than other algorithms. Also AES has advantage over the other 3DES and DES in terms of throughput and decryption time. 3DES has least performance among all mentioned algorithms.

Apoorva et al. [4] compared most common symmetric cryptography algorithms: AES, TWOFISH, CAST-256 and BLOWFISH. The comparison took into consideration the behavior and performance of algorithms when different data loads were used. The comparison was made on the basis of these parameters: speed, block size, and key size. It was concluded that blowfish is superior to other algorithm as it takes less time. Although when the data size was very small this difference was not clearly visible. But for file having size greater than 100 KB, it was very clearly visible.

Abdul et al. [1] discussed six most common encryption algorithms such as AES (Rijndael), DES, 3DES, RC2, BLOWFISH and RC6. These algorithms were compared and performance was evaluated. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. It was concluded that there is no significant difference when the results are displayed either in Hexadecimal Base encoding or in Base 64 encoding. Secondly in the case of changing packet size, it was concluded that BLOWFISH has better performance than other common encryption algorithms used, followed by RC6. Also in the case of changing data type such as image instead of text, it was found that RC2, RC6 and BLOWFISH has disadvantage over other algorithms in terms of time consumption. Also, it was found that 3DES still has low performance compared to algorithm DES. Finally in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption.

Thakur et al. [20] discussed a fair comparison between three most common symmetric key cryptography algorithms: DES, AES and Blowfish. The main concern was the performance of the algorithms under different settings, the presented comparisons takes into consideration the behavior and performance of the algorithms when different data loads are used. The comparison was made on the basis of these parameters: speed, block size, and key size. Simulation program was implemented using java programming. It was concluded that blowfish has better performance than other common encryption algorithms used.

Marwaha et al. [10] discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic

algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

Alam et al. [3] discussed performance and efficiency analysis of different block cipher algorithms (DES, 3DES, CAST-128, BLOWFISH, IDEA and RC2) of symmetric key cryptography. Block cipher algorithms has been compared based on the factors: input size of data(in the form of text, audio and video), encryption time, decryption time, throughput of encryption and decryption of each block cipher and power consumption. It was concluded that 3DES has more power consumption and less throughput than the DES due to its triple phase characteristics. Throughput of CAST-128 was better than DES, 3DES and IDEA. RC2 was faster for smaller sizes of input data as compared to BLOWFISH algorithm because it has only one P-Box for key expansion loaded into memory as compared to BLOWFISH which has one P-Box and four S-Boxes. Throughput value of BLOWFISH was greater than 3DES, DES, CAST-128, IDEA and RC2. Power consumption value of BLOWFISH was least. 3DES having the least throughput and maximum power consumption value as compared to all block cipher discussed in this paper. From the experimental results it was also concluded that by taking input data in the form of text, audio as well as video throughput of encryption and decryption of all block ciphers discussed here was almost same in all three forms of data. It was concluded by analyzing Encryption/Decryption time, Encryption/Decryption throughput and power consumption value that BLOWFISH has better performance and efficiency than all other block ciphers compared in this paper.

Saini [12] make a performance analysis of various algorithms- DES, AES, RC2, Blowfish, 3DES and RC6. It was concluded from the simulation outcomes that best algorithm are those that are well known and well documented because they are well tested and well studied. A good cryptographic system strikes a balance between what is possible and what is acceptable.

V.COMPARISON ANALYSIS

A. COMPARISON OF VARIOUS CRYPTOGRAPHY TECHNIQUES

The comparison of all above cryptography techniques is given in Table 1

Table 1: Comparison of all above cryptography techniques

Algorithm	Created By	Year	Key Size	Block	Round	Structure	Flexible	Features
DES	IBM	1975	64 bits	64 bits	16	Festial	No	Not Strong Enough
3DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security
AES	Joan Daeman & Incent Rijmen	1998	128,192,256 bits	128 bits	10,12,14	Substitution Permutation	Yes	Replacement for DES, Excellent Security
BLOWFISH	Bruce Schneier	1993	32-448	64 bits	16	Festiel	Yes	Fast Cipher in SSL
RC4	Ron Rivest	1987	Variable	40-2048	256	Festiel Stream	Yes	Stream Cipher
RC2	Ron Rivest	1987	8,128,64 by default	64 bits	16	Festiel	-	Stream Cipher
TWOFISH	Bruce Schneier	1993	128-256	128 bits	15	Festial	Yes	Good Security

Serpent	Anderson Lars	1998	128-256	128 bits	32	Substitution Permutation	Yes	Good Security
IDEA	James Massey	1998	128 bits	64 bits	8.5	Substitution Permutation	No	Not Strong enough
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128 bits	1	Public Key Algorithm	No	Excellent Security and Low Speed
RC6	Ron Rivest et.al	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	Good Security

VI. **Conclusion**

Text data plays an important role in lives and they are used in many applications in our day to day lives. Therefore it is necessary to affirm the integrity and confidentiality of the data that being transmitted. Some of the encryption techniques are discussed that plays an important role in data transmission. In this paper a survey of some important cryptography algorithm is provided in last decades. This encryption methods are studied and analysed well to promote the performance of encryption methods. Each technique is unique in its own way and this make it suitable for its many application. Everyday new techniques are evolving hence fast and secure conventional encryption techniques work with high security rate. This survey provide a way to design and invent a new and fast encryption algorithm compare with the existing algorithm.

VII. Future Scope

In this paper we analyze that the process of encryption and decryption is perform by using DES, 3DES, CAST, Serpent, RC4, RC6, UMARAM, UR5 and Blowfish algorithms. In future we will apply and implement these processes for secure and better communication.

References

[1] Chia Long Wu , Chen Hao Hu ,"Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", Innovations in Bio-Inspired computing and Applications(IBICA), 2012, pp. 307 – 311.

[2] Qing Liu, Yunfei Li, Lin Hao, "On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), 2010, pp.533-536.

[3] Mandal, B.K. , Bhattacharyya , Bandyopadhyay S.K. , "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm ", Communication Systems and Network Technologies (CSNT), 2013, pp. 453 – 461.

[4] Wang, Suli , Liu, Ganlai , "File encryption and decryption system based on RSA algorithm", Computational and Information Sciences (ICCIS), 2011, pp. 797 – 800.

[5] Da Silva, J.C.L ,"Factoring Semi primes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2010, pp.182–183.

[6] Geethavani, B. , Prasad, E.V. Roopa, R. "A new approach for secure data transfer in audio signals using DWT" , pp.1-6, Sept 2013.

[7] Nagar, S.A. , Alshamma, S. , "High speed implementation of RSA algorithm with modified keys exchange", Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) , Page(s): 639 – 642 , 2010.

[8] Chong Fu , Zhi-liang Zhu , "An Efficient Implementation of RSA Digital Signature " , Wireless Communications, Networking and Mobile Computing, Oct. 2008 , pp.1-4.

[9] Li Dongjiang ,Wang Yandan , Chen Hong, "The research on key generation in RSA public- key cryptosystem", 2012, pp. 578–580.

[10] Turki Al-Somani ,Khalid Al-Zamil , "Performance Evaluation of Three

Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems".

[11] Hongwei Si , Youlin Cai , Zhimei Cheng , "An Improved RSA Signature Algorithm Based on Complex Numeric Operation Function", Challenges in Environmental Science and Computer Engineering (CESCE), 2010 , pp.397–400.

[12] Wenxue Tan ,Wang Xiping , Jinju Xi , Meisen Pan , "A mechanism of quantitating the security strength of RSA key", Electronic Commerce and Security (ISECS), 2010, Page(s): 357 – 361.

[13] Dhakar, R.S. ; Gupta, A.K. ; Sharma, P., "Modified RSA Encryption Algorithm (MREA)", Advanced Computing & Communication Technologies (ACCT), 2012, pp.426–429.

[14] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "

[15] Challa Narasimham, Jayaram Pradhan," Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files" , Journal of Theoretical and Applied Information Technology, pp. 55-59, 2008.

[16] Abdel-Karim Al Tamimi, Swati.," Performance Analysis of Data Encryption Algorithms " , International Journal of Advanced Research in Computer Science and Software Engineering 3(2), pp. 147-149 , February – 2013.

[17] Nidhi Singhal1, J.P.S.Raina2, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technologypp.177-181, Aug 2011,

[18] Pratap Chandra Mandal, " Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish ", Journal of Global Research in Computer Science Department of Computer Application, vol 3, pp 67-70, August 2012.

[19] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.

[20] Deepak Kumar Dakate, Pawan Dubey , " Performance Comparison of Symmetric Data Encryption Techniques " , International Journal of Advanced Research in Computer Engineering & Technology , Volume 3, No. 8, August 2012, pp . 163-166.

[21] Shashi Mehrotra Seth, Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, pp.192-192 , June 2011.

[22] Gurjeevan Singh , Ashwani Kr. Singla , K.S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks" , International Journal Computer Applications (0975 – 8887) Volume 44 – No11, pp.23-26 , April 2012.

[23] Agarwal, R. , Dafouti, D., Tyagi, S. "Peformance analysis of data encryption algorithms ", Electronics Computer Technology (ICECT), 2011 3rd International Conference , vol.5 , April 2011, pp. 399 - 403 .

[24] Ramesh, A. et.al.,, "Performance analysis of encryption algorithms for Information Security " Circuits, Power and Computing Technologies (ICCPCT),March 2013 , pp. 840 - 844

[25] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[26] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[27] Alam Md Imran, Khan Mohammad Rafeek. "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, pp.713-720.

[28] Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

[29] Cornwell Jason W, "Blowfish Survey", Department of Computer science, Columbus State university, Columbus, GA, 2010.

[30] Dhawan Priya, "Performance Comparison: Security Design Choices", Microsoft Developer Network October 2002.

[31] Forouzan Behrouz A., "Data Communications & Networking", Fourth Edition, 2008, New York: Tata McGraw- Hill.

[32] Jeeva AL, Palanisamy, Dr. V., Kanagaram K. "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms ", International Journal of Engineering Research and Applications(IJERA), Volume 2, Issue 3, May-June 2012, pp. 3033-3037.

[33] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.
[34] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.
[35] Nadeem Aamer, "Performance Comparison of Data Encryption Algorithms", Oct 2008.
[36] Saini Bahar, "Survey On Performance Analysis of Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014, pp. 1-4.
[37] Schneier B., "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.
[38] Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.
[39] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 2, pp.321-326.
[40] Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communications, Vol. 2, No.1, January-June 2011, pp. 125-127.
[41] Stallings William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.
[42] Tamimi A. Al., "Performance Analysis of Data Encryption Algorithms", Oct 2008.
[43] Tanenbaum Andrew S., "Computer Networks", Third Edition, Prentice Hall India, 2000.
[44] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", IJETAE, vol. 1, Issue 2, DEC. 2011, pp. 6-12.