Proceedings of the SMART–2016, IEEE Conference ID: 39669
5th International Conference on System Modeling & Advancement in Research Trends, 25th–27th November, 2016
College of Computing Sciences & Information Technology, Teerthanker Mahaveer University, Moradabad, India

DES: The Oldest Symmetric Block Key Encryption Algorithm

Mukta Sharma[1] and Dr. R.B. Garg[2]
[1]Research Scholar, TMU, University of Delhi
[2]Ex-Professor, University of Delhi
E-mail: [1]m.mukta19@gmail.com, [2]garg1943@gmail.com

***Abstract*—Cryptography is a part of Cryptology; which deals with reading, writing and breaking of code. Cryptography is a technique used to camouflage the message into some unreadable text. It is a way of ensuring security when transmitted through an insecure channel. An insecure channel is that channel, where unethical hacking, tampering of information is easily possible. Encryption is a process which enciphers the plain/ original text into cipher text. Hackers will hack the data/ information/ message but will not be able to retrieve the original text because of encryption. This paper deals with one of the most famous and oldest symmetric key encryption algorithm "DES-Data Encryption Standard." It highlights the primary flow, history, implementation, significant drawbacks, etc.**

Keywords: Asymmetric Cryptography, Cipher Text, DES, Plain Text, Symmetric Cryptography

I. INTRODUCTION

The modern era has given society a benefit of staying connected. There is a need for more security because of lot more data in available online nowadays. Encryption of data has been used since ages & is now used more extensively. Essential factors of encryption are data authentication and privacy. Cryptography is a way of writing secretly. Two Greek words Kryptos-Secret, hidden and Graphite-Writing have been combined to form this new mandate. The concept of encryption is ancient it has begun thousands of years ago. Cryptography, the term was coined in 1658 by Thomas Brownie [11]. In the past much before the internet; cryptography was used by the military to protect valuable information. Primarily cryptography can be done in two ways. One using a unique or single key to encipher and decipher the text, this method is called conventional encryption or symmetric key encryption or Private Key. The symmetric key was the only way of enciphering before the 1970s. Asymmetric key encryption algorithm also popularly said as public key encryption. This concept uses a set of keys one public key known to all users who wish to send the information and the other is the private key which is known only to the recipient with which recipient can decipher the received messages.

Symmetric Key Encryption can be performed using Block Cipher or Stream Cipher. Stream Cipher takes one bit or one byte as an input, process it and then convert it into 1bit or 1-byte cipher-text. Like RC4 is a stream cipher. It is used in every mobile phone whether that phone is with or without the internet. Block cipher as the name suggests it executes on a single block at a time and so on. It works on a fixed block size as an input and fixed block size as an output (ciphertext). Like DES, 3DES are a 64bit block cipher.

Key Elements of Cryptography are as follows:[7][32]

- Plain Text-the authentic or the individual message which sender sends as an input.
  Key-The secret key has an indispensable role. For the processing of an algorithm, the key is essential and given as an input. The key has to be strong; else the algorithm can be easily decrypted if the key is weak. A Key size ensures security.
- Encryption-Encryption is a way of converting the original message to scrambled text.
- Cipher Text-The text in a format that it is unreadable for any unintended user.
- Decryption-Decryption is a way of retrieving the authentic or original text (reverse of encryption algorithm).

II. DES

Data Encryption Standard developed in March 1975 by IBM was later adopted in 1977 by NIST. DES is the first commercial-grade modern algorithm with all specified implementations defined by FIPS 46–2 (Federal Information Processing Standard 46) [17]

III. HISTORY OF DES

DES is a block cipher depicted in Fig. 1 it takes 64-bit block size as an input (Plain Text) and gives 64 bit as an output (Cipher Text). After the success of LUCIFER, DES algorithm was developed. LUCIFER was designed by Horst Feistel, IBM, 1971[8]. Lucifer uses 64bit block size, and 128 bitkey, wherein DES uses 64bit block size and 56-bit key size which was 72 bit less than LUCIFER [3][25]. DES was adopted as a federal standard on 23rd November 1976 [17].

 ISBN: 978-1-5090-3543-4

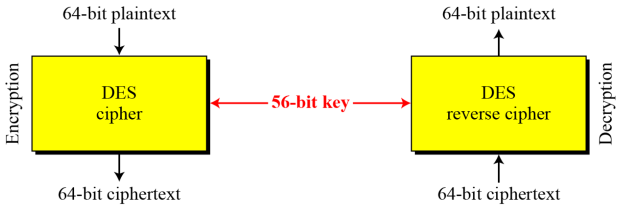

Fig. 1: DES is a Block Cipher [7]

With a goal to commercialize encryption, an encryption algorithm named DES was designed. The prime concern was hardware based therefore the key size was reduced to fit on a single chip. Tuchman, Carl Meyer, and many other researchers from not only IBM but also from National Security Agency (NSA) designed DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard (FIPS) [17]. Keeping the following in mind DES was designed:

a. *Feistel Network*: A concept which was conceived by Horst Feistel in 1973. In Feistel network, it divides the plaintext block into two halves, L0 and R0. DES follows Feistel network; a 64-bit original data is split into two halves of 32 bit each. For producing the ciphertext total 16 rounds are performed on the data (L0, R0) [32].

b. *Confusion & Diffusion:* Claude Shannon also known as Father of Information Theory gave two operations "Confusion and Diffusion." To build a secure encryption algorithm, the concept of confusion and diffusion should be concatenated. The process of concatenating confusion-diffusion is called as "Product ciphers" [27]. Confusion, Diffusion leads to Avalanche effect.

According to Claude Shannon, the concepts of confusion and Diffusion will make the cipher unbreakable. The information or message is statistically scattered and replaced which becomes quite confusing and challenging for an attacker to crack. Diffusion can be accomplished using permutations (rearranging) and transpositions [27]. The complex substitution (replacing) algorithm is used to attain Confusion [27].

A suitable encryption algorithm for ensuring better security should implement Confusion and Diffusion numerous times.

Primary concern around DES-DES faces major criticism since the adoption:

- DES executes the code on a single chip to become a commercial product for encryption; has compromised on the Key size. The small key size of-56 bit was prone to various attacks like brute force.
- Mysterious S-box: design criteria were kept hidden-The eight S-Boxes being the weak points are kept hidden from all and have never been specified o published. It's speculated that the weakness in S-boxes makes the life of Cryptanalysts much easier to exploit DES. [7][25]

IV. Working of DES

The primary structure of DES is shown in Fig. 2. DES accepts 64-bit block size as an input (Plain Text), and after execution of the algorithm, a 64-bit cipher is produced. DES receives 64 bits, each of which may be either 0 or 1 as DES works in binary.

a. *Encryption Process:* After getting the information the first step is to permute the data using initial permutation as depicted in Table 1. DES uses the concept of confusion and Diffusion to enhance security. Diffusion is attained by using Permutation which rearranges the bits. As shown in below Table, the first bit after Initial Permutation will be the 58th bit of the Input, 2nd bit after IP would be the 50th bit of the data and so on. The data would be arranged according to the Table given below.

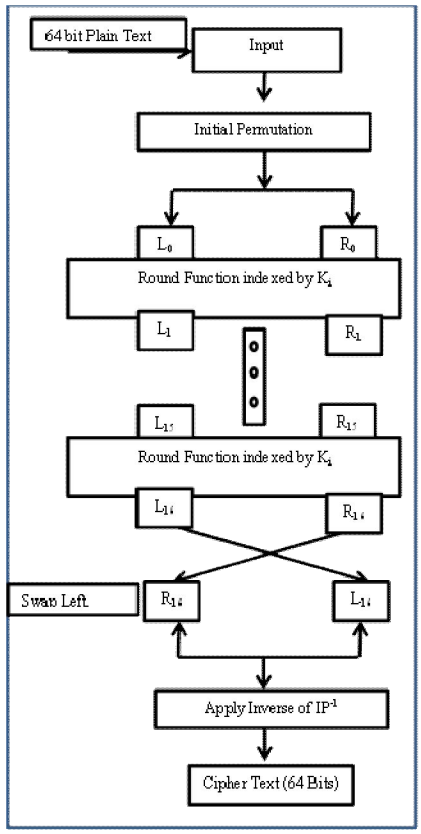

Fig. 2: Working of DES [25]

TABLE 1: INITIAL PERMUTATION (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

A. Key Generation

Initially, the Key size is 64 bits which are reduced to 56 bits after removing all parity bits i.e. every 8th bit (8, 16, 24, 32, 40, 48, 56, and 64). Later Permuted Choice-1 matrix given below in Table 2 is used to permute the key. For instance "57", is the first entry in Table 2; which means that the first bit of the permuted key will have the value of the 57th bit of the original key K. The 4th bit of the actual key will become the last element of the permuted key and so on.

TABLE 2: PERMUTED CHOICE-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Next step is to divide 56 bit permuted key into equal halves of 28 bit each (C_0, D_0). The first half comprising of 1-28 bits, and the second half consisting bits from 29-56. For 16 rounds, 16 sub-keys have to be defined; Cn and Dn, 1<=n<=16 [7]. Each pair of blocks Cn and Dn are formed from the previous pair Cn-1 and Dn-1, respectively, for n = 1, 2,..., 16, using the following schedule of "circular left shift" of the previous block [25] [32].

Left Circular Shift is based on the rounds like 1, 2, 9 and 16 shift 1left bit. Rest all rounds (3, 4, 5, 7, 8, 10, 11, 12, 13, 14 and 15) move 2 bits; which finally makes 28bit (4*1+ 12*2= 28 bits).

Fig. 3 depicts the entire key generation flow. Key size is 56 bits, but Permuted Choice-2 refer Table 3 has only 48 bits. Therefore 16 subkeys of 48 bits will be acquired.

TABLE 3: PERMUTED CHOICE-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

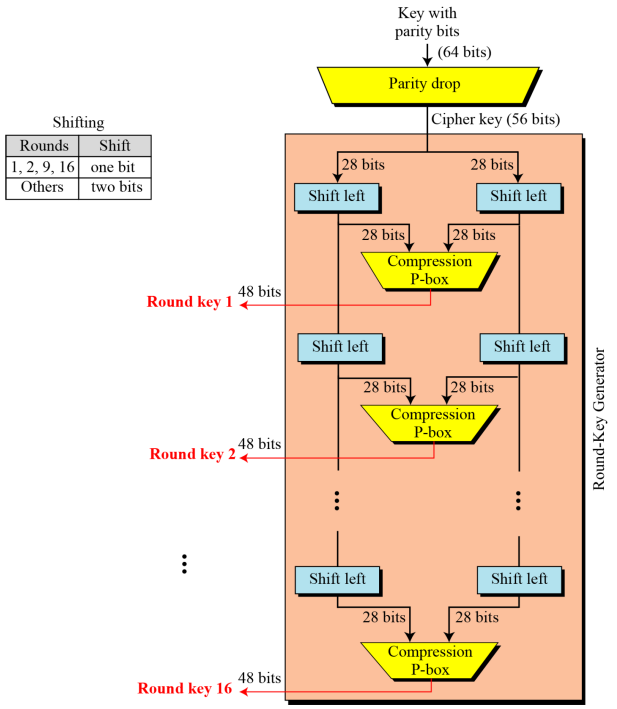

Fig. 3: Key Generation

a. Round Function-16 iterations, for 1<=n<=16 execute function (f). Two blocks are required to process the function (f). One is data block, and the other is key-As already discussed 64-bit Plain text is divided into the 32-bit data block.

Sub key of 48 bits is required to produce a block of 32 bits.

As highlighted in Fig. 4, the first 32 bits of the right block will be passed as an input to the left block (Ln = Rn-1). Second step [Rn = Ln-1 + f(Rn-1,Kn)] would initiate with R block of 32 bits (4*8). R Block needs to be expanded to 48 bits (6*8) so that XOR with the subkey is possible. XOR is also known as Modulo 2.

32 bit are expanded to 48 bits, refer to fig. 5 for the expansion procedure. One previous bit is added to the front or as the first bit, and one next bit is added as the last bit. For instance, 1234 will be expanded as 32 (a previous bit)1234 and 5(next bit).

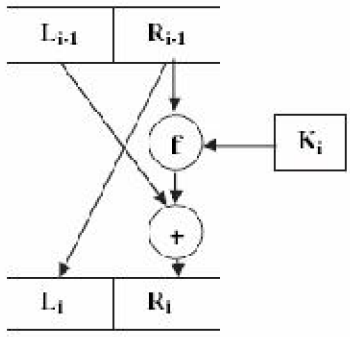

Fig. 4: DES Rounds

The function is explained in Fig. 6. After Expansion the result will be XOR with the subkey of 48 bits, the result is 48 bits (8 groups of 6 bits i.e. 8*6=48). S-boxes are used to suppress 48-bit data back to 32 bit. Each group of six bits will give us a location in a different S-box.

Each S-Box will generate a 4-bit output (4*8=32). To fetch the value from S-Boxes, the first and last bit of a six-bit block are used for the row. 2nd 3rd 4th and 5th bits which are in the mid of the block will be representing the column. Now these rows and columns are used to locate the value in the S-Box Table and convert it into a hexadecimal value. S-Box Table is represented by 4 rows (ranging 0 to 3, with base 2 i.e. 00 to 11) & 16 columns (ranging 0 to 15, i.e. 0000 to1111).

b. Decryption in DES-Decryption with a symmetric key algorithm is the same as Encryption process. It is just the inverse of encryption. Decryption can be easily attained just need to reverse the order of the subkeys. [32][7][25]

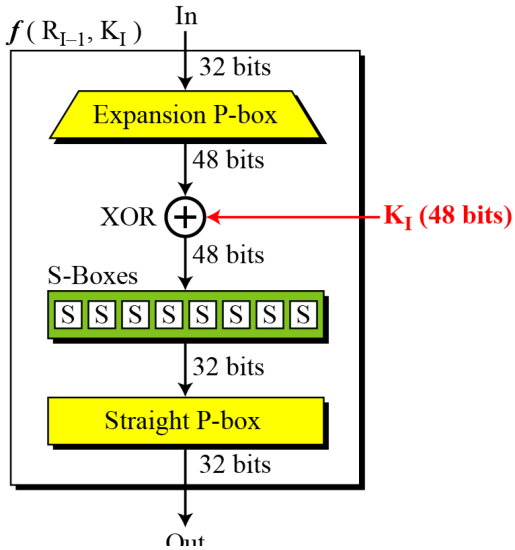

Fig. 6: DES Function [7]

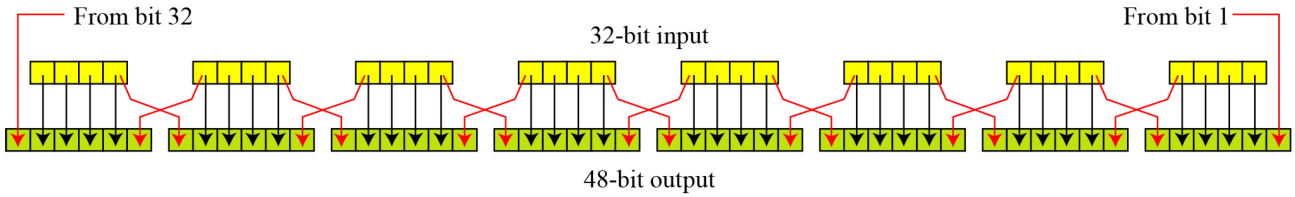

Fig. 5: Expansion Permutation [7]

V. DES Analysis

TABLE 4: PERFORMANCE CRITERIA BASED ON EXISTING STUDIES

Research	Performance Factors
(Singh *et al.* 2014)	Time Complexity [30].
(Sindhu, G., Krithika, P., 2015).	Time, Different File Size [29].
(Mandal, P.C., 2012).	Throughput, Battery and Power Consumption [13].
(Elminaam *et al.*, 2008)	CPU process time, Encryption time, and battery power [4].
(Mushtaque, A, M., 2014).	Space Complexity [15].
(Elminaam *et al.*, 2010)	Time Consumption, Throughput, Different Data Types, Packet size, Power Consumption [5].
(Ramesh, G., UMARANI, R.,, 2012)	Throughput, Battery and Power Consumption, on file type as Images [21]
(Lemma. A, 2015)	Throughput, Time Consumption, CPU process time, CPU clock cycles and battery power [12].
(Mittal, M., 2012).	Different Hardware and Operating System [14].
(Karthik, S., 2014).	Time, Data block, Modes [10]
Tripathi, S.K., Lilhore, U.K. (2016)	Block size, Key size, Avalanche effect [34]
(Sandhu, G.S., Verma, V., 2013).	Pearsonian Chi-Square Value, Payload capacity, Robustness against statistical attacks, manipulations, Independent File Types [29]
(Alam, I. M., Khan, R. M., 2013).	Throughput, Power Consumption, Encryption Time [1]
(Pavithra, S., Ramadevi, E., 2012).	Throughput Analysis based on file type [19]
(Seth, 2011)	Computation time, memory usage, output bytes, throughput time [26]
(Salama. D, 2009)	Power consumption for wireless devices [22]
(Nadeem and Javed, 2005)	Different data, different data sizes, different hardware platforms [16]
(Singhal *et al.*, 2011)	CPU time, encryption time, memory usage [31]
(Thakur and Kumar, 2011)	Speed, block size, key size [33]
(Olagunju and Soenneker, 2012)	Data types-audio, video, text [18].
(Vijayalakshmi and Raja, 2012)	Memory size for both the process with different word lengths, key sizes, Encryption time, Decryption time [35].
(FARAH *et al.*)	Encryption/decryption time, memory usage, throughput over variable test file, private key sizes [6].
(Ananthi, B., Priya, V., 2014)	Using MATLAB power consumption, Throughput [2]
(Sharma, Kumar, Lakshmi, 2013)	Video Encryption [28]
(Salama. D, 2011)	Throughput, ▪Battery power, Encryption time Transmission time in cases like video file, wireless etc. [23]
(Karova, M., Todorova, M)	Different File type with different sizes [9]

For analysing the strength of any block cipher algorithm the following desirable properties need to be tested: avalanche effect and the completeness.

- Avalanche Effect is a required feature of the cryptographic algorithm. It means that by changing only one bit (small change), there is a significant shift in the cipher; so that it was difficult to perform an analysis. [7] [25].

Avalanche Effect= Number of flipped bits in ciphered text/ Number of bits in ciphered text [34]

- Completeness Effect-each ciphertext bit is dependent on various plain text bits. [7]

a. *Performance Criteria's:* The criteria's to evaluate the performance are Architecture, Scalability, Flexibility, Security, and Limitations. The performance of encryption algorithms is based on various parameters like Encryption Time, Decryption Time, Speed, Usage, CPU Utilization, Key size, Block Size, Security, etc. Various researchers have critically analyzed DES based on the data files, file size, etc.

VI. DES Security

DES, being the first adopted and most modern block cipher has undergone an in-depth scrutiny. Critics have found some weaknesses in DES-like Weaknesses in S-boxes, P-boxes, and Key. Some attacks like Brute-force, differential cryptanalysis, and linear cryptanalysis are among the attempted attacks [25] [7] [32].

TABLE 5: ATTACKS ON DES IN THE PAST

Year of Attack	Attacks on DES
1977	Diffie & Hellman designed a machine to break brute force attack: estimated cost $20Milion and 12 hours to break
1981	Estimated breakable in 2 days by $50M machine
1990	Israeli researchers-Biham & Shamir propose differential cryptanalysis (247 chosen cipher texts)
1993	• An very efficient key search machine was designed by Mike Wiener: Average search requires 36h. Costs: $1.000.000 • Matsui, a Japanese researcher proposed linear cryptanalysis (2^{43} chosen cipher texts)
1996	56 bit ($10Million/21 min, 10k$/556 days, 400$/38 years)
Jun. 1997	DESCHALL Project-Broken in 96 days by 70000 machines testing 7 billion keys
Feb. 1998	DES was broken in just 39 days using distributed search
Jul. 1998	DES Challenge II--2 broken, key search machine Deep Crack built by the Electronic Frontier Foundation (EFF): 1800 ASICs with 24 search engines each, Costs: $250K finding key in 4.5 days.
Jan. 1999	Broken in 22h 15min (Deep Crack) +100000 machines, testing 245 billion keys
2006-2008	COPACOBANA a reconfigurable key search machine was developed at the Universities in Bochum and Kiel (Germany). It uses 120 FPGAs to break DES in just 6.4 days (avg.) at a cost of $10 000.

VII. DES Usage in the Real World

Being the first commercial encryption algorithm, DES got the first mover advantage. DES was used by all financial transactions of the U.S. and was utilized by the government for better security. In fact, was used for important communications for the safety reasons. It is being used by Digital right management, US [25].

Triple DES uses the same structure of DES algorithm. It is more secure as it uses the concept of 3 keys that is 56*3=168 keys, 16*3=48 rounds. Microsoft uses DES for its various products like OneNote, Outlook 2007 and System Center Configuration Manager 2012, etc. Triple DES is being used to protect password, user content and system data.

VIII. Conclusion

DES being the first commercially accepted encryption algorithm was used at numerous places to provide security. DES is based on Feistel network, used Shannon principle of confusion and diffusion to improve safety. DES was designed keeping the hardware in mind. DES has compromised on the key size of 56 bit. Reduced key size has made DES vulnerable against Brute force attack [32]. DES being the pioneer was attacked by many attackers.

Differential cryptanalysis requires 2^{47} chosen plaintexts to break the full 16 rounds. Similarly, 2^{43} known plaintexts attack was reported for Linear Cryptanalysis and so on. DES is now vulnerable and is not used by military or government. The bottom line is that DES is not used to protect security and privacy of sensitive or confidential data.

References

[1] Alam, I. M., Khan, R. M., (2013). Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3(10).

[2] Ananthi, B., Priya, V. (2014). Comparative Analysis of Image Encryption and Decryption for Securing Medical Images. Journal of NanoScience and NanoTechnology, Vol. 2, Issue 6, pp. 636-639.

[3] D.K. Branstad, J. Gait, and S. Katzke, (1977). Report on the Workshop on Cryptography in Support of Computer Security. NBSIR 77–1291, National Bureau of Standards.

[4] Elminaam, A., Abdual, D. S., Kader, H.M., and Hadhoud, M.M. (2008). *Performance Evaluation of Symmetric Encryption Algorithms.* IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12.

[5] Elminaam, A., Abdual, D. S., Kader, H.M., and Hadhoud, M.M. (2010).Evaluating The Performance of Symmetric Encryption Algorithms. International Journal of Network Security, Vol.10(3), PP.213-219.

[6] Farah, S., Javed, M. Y., Shamim, A. & Nawaz, T. An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms.

[7] Forouzan, B.A., & Mukhopadhyay, D. (2010). Cryptography and Network Security. NewDelhi, India: Tata McGraw-Hill.

[8] H. Feistel, W.A. Notz, and J.L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications", Proceedings on the IEEE, v. 63, n. 11, 1975, pp. 1545-1554.

[9] Karova, M., Todorova, M. Comparative Analysis of Algorithms for Communication Encryption. Mathematics and Computers in Sciences and Industry.

[10] Karthik, S, Muruganandam. A.,(2014). Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System. International Journal of Scientific Engineering and Research (IJSER), Vol. 2(11).

[11] L. Bauer (2010), Decrypted Secrets: Methods and Maxims of Cryptology, Neal Koblitz, SIAM Review, Vol. 52 (4).

[12] Lemma. A., Tolentin. M., Mehari. G., (2015). Performance Analysis on the Implementation of Data Encryption Algorithms Used in Network Security. International Journal of Computer and Information Technology (ISSN: 2279–0764) Volume 04–Issue 04.

[13] Mandal, P.C., (2012). Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. Journal of Global Research in Computer Science, Volume 3, No. 8.

[14] Mittal, M. (2012). Performance Evaluation of Cryptographic Algorithms. International Journal of Computer Applications (0975–8887) Volume 41–No.7.

[15] Mushtaque, A, M. (2014). Comparative Analysis on Different parameters of Encryption Algorithms for Information Security. International Journal of Computer Sciences and Engineering Vol.-2(4), pp (76-82).

[16] Nadeem, A. & Javed, M. Y. (2005). A performance comparison of data encryption algorithms. Information and communication technologies. First international conference on, 2005. IEEE, 84-89.

[17] NIST FIPS PUB 46-3. "Data Encryption Standard. Federal Information Processing Standards, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., 1977.

[18] Olagunju, A. & Soenneker, J. (2012). A Performance Analysis Model for Cryptographic Protocols. Available: http://www.iiisci.org/journal/CV$/sci/pdfs/HHB799EQ.pdf [Accessed 30 Nov 2012].

[19] Pavithra, S., Ramadevi, E. (2012). Throughput Analysis of Symmetric Algorithms. Int. J. Advanced Networking and Applications, Volume:04 Issue:02 Pages: 1574-1577.

[20] Protocols, Algorithms, and Source Code in C.John Wiley & Sons.

[21] Ramesh, G., UMARANI, R., (2012). *Performance Analysis of Most Common Symmetrical Encryption Algorithms*. International Journal of Power Control Signal and Computation(IJPCSC), Vol3. No1.

[22] Salama. D, E. A., Hatem M. A. K and Mohie M. H (2011). Studying the Effects of Most Common Encryption Algorithms. International Arab Journal of e-Technology, Vol. 2, No. 1.

[23] Salama.D, E. A., Hatem M. A. K and Mohie M. H (2009). Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices. International Journal of Computer Theory and Engineering, 1, 343-351.

[24] Sandhu, G.S., Verma, V. (2013). Comparing Popular Symmetric Key Algorithms Using Various Performance Metrics. International Journal of Advance Research in Computer Science and Management Studies, Vol. 1(7).

[25] Schneier, B. (1996). Applied Cryptography.

[26] Seth, S. M. Mishra, R. (2011). Comparative Analysis of Encryption Algorithms For Data Communication, Vol. 2. Issue, 2, pp. 292-294.

[27] Shannon, Communication theory of secrecy systems, Bell System Technical Journal, vol 28,pp 656-715, 1949.

[28] Sharma, S., Kumar, P., Lakshmi, P., (2013). A Study Based on the Video Encryption Technique. International Journal of P2P Network Trends and Technology-Volume3, Issue1.

[29] Sindhu, G., Krithika, P. (2015). Analysis and comparison of symmetric key algorithms (Blowfish, DES, TEA, IDEA) in cryptography. IJSART-Volume 1 Issue 11–NOVEMBER 2015.

[30] Singh, V., Dhiman, H., Khatkar, M. and Nida (2014). A Comprehensive Study of Time Complexity of Various Encryption Algorithms. International Journal of Advances in Engineering & Technology, May, 2014.

[31] Singhal, N. R. &Jps (2011). Comparative Analysis of AES and RC4 Algorithms for Better Utilization. International Journal of Computer Trends and Technology.

[32] Stallings, W. (2011). Cryptography and Network Security: Principles and Practice. US, USA: Pearson.

[33] Thakur, J. & Kumar, N. (2011).DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, 6-12.

[34] Tripathi, S.K., Lilhore, U.K. (2016). Survey on Performance Comparison of Various Symmetric Encryption Algorithms, International Journal of Recent Trends in Engineering & Research, Vol.2 (4).

[35] Vijayalakshmi, P. R. & Raja, K. B. (2012).Performance analysis of RSA and ECC in identity-based authenticated new multiparty key agreement protocol. International Conference on Computing, Communication and Applications, 1-5.

