DES and AES Performance Evaluation

Bawna Bhat
School of Computer Science and Engineering
Galgotias University
Greater Noida, UP, India
bhatbawna@gmail.com

Abdul Wahid Ali
School of Computer Science and Engineering
Galgotias University
Greater Noida, UP, India
wahidmalik89@gmail.com

Apurva Gupta
School of Computer Science and Engineering
Galgotias University
Greater Noida, UP, India
erapurvagupta@gmail.com

***Abstract*— In these days use of digital data exchange is increasing day by day in every field. Information security plays very important role in storing and transmitting the data. When we transmit a multimedia data such as audio, video, images etc. over the network, cryptography provides security. In cryptography, we encode data before sending it and decode it on receiving, for this purpose, we use many cryptographic algorithms. AES and DES are most commonly used cryptographic algorithms. AES provides the encryption to secure the data before the transmission and DES also provides security as AES. In this paper we discussed AES and DES and their comparison using MATLAB software .After applying AES and DES, we compare their result on the basis of avalanche effect, simulation time and memory required by AES and DES.**

Keywords—— AES; DES; Cryptography; entropy.

I. INTRODUCTION

Cryptography [1] is the science of keeping message secure. The method, in which we disguising a message in such a way so that its substances are kept are encryption and encrypted message, is cipher text. The process of diversion cipher text back in plain text is decryption. The terms encipher and decipher are already used as standards by ISO 7498-2. It gives protection to the message so that an unauthorized party cannot see or alter our message [2]. In cryptographic some symbols are used to denote most things like as P is used to represent plaintext, M is used for message, plain text is like a stream of bits, text file, a digitized voice, a digital video image may be and C is used to denote cipher text. Cipher text is of same size or more than size of message M. Cipher text is a binary (M is smaller when encryption is combined with compression C).

Brief introduction is discussed in section I. In Section II, overview of cryptography and encryption techniques are discussed. Experimental design is discussed in section III. In section IV experimental result and analysis and section V presents the conclusion of the paper.

II. OVERVIEW OF CRYPTOGRAPHY AND ENCRYPTION TECHNIQUES

A. Cryptography and Classification

Cryptography is the protecting technique of data from the unauthorized party by converting into the non-readable form. The main purpose of cryptography is maintaining the security of the data from third party. The classification of cryptography on the basis of key based algorithm, there are following two types of algorithms such as: (i) symmetric key based algorithm, sometimes known as conventional key algorithm and (ii) asymmetric key based algorithm, also known as public-key algorithm. Symmetric algorithm can be further divided into two types. Classification of key based algorithms is discussed in Figure-1. Some operate on the plaintext a single bit at a time; these are called stream algorithm or stream ciphers [3]. Others operate on the plaintext in groups of bits. In block algorithm or the block cipher, we use blocks and these are group of bits.

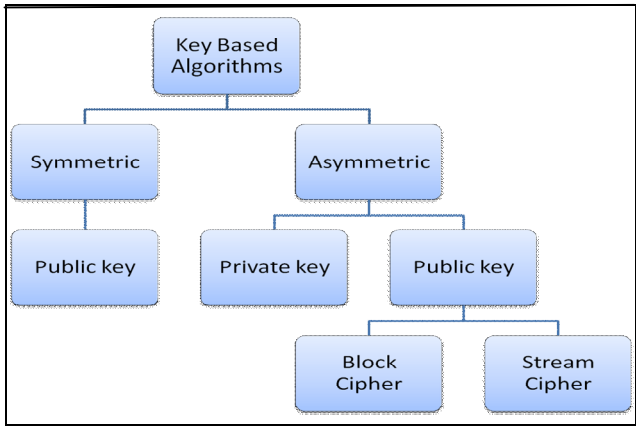

Figure-1 Classification of Key based Algorithms

B. Data Encryption Standard

Data Encryption Standard is a symmetric key algorithm for encrypt the data, to secure from attacker or unauthorized party. DES provides the influence in security world to protect the information. National bureau of standards firstly adopt the Data Encryption Standard (DES) in year 1997, nowadays is called Federal Information Processing Standards.

In DES [1][9], the key size is 56 bits. In fact, the 56-bit key is divided into eight 7-bit blocks and additional 8th odd parity bit is further added to every block (i.e. to obtain odd number of 1in every 8-bit block, 0 or 1 if further added to it)[4].By using the 8 parity bits for rudimentary error detection, a DES key is actually 64 bits in length to avoid randomness, it is 56 bit for computation. After perform the splitting the bits into several blocks, perform the shift left and right operations to

improve the privacy into information and then Ex-Or operation BJP Boxes and S-Boxes, finally get the encrypted data to maintain the privacy. The block diagram of DES shows in Figure-2.

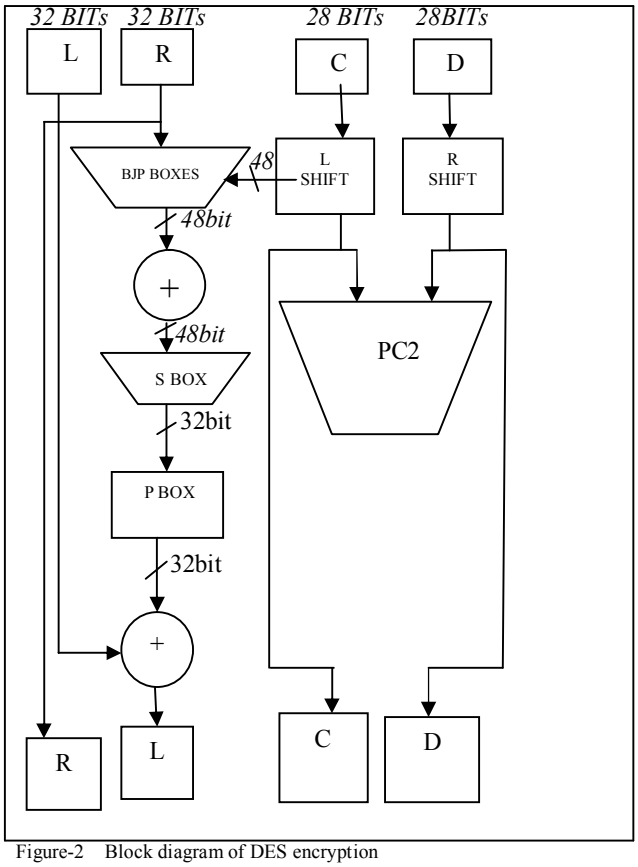

Figure-2 Block diagram of DES encryption

C. Advanced Encryption Standard

As DES key is small in size and its processor power has less technological advancement is Advanced Encryption Standard (AES)[5][9]. Advanced Encryption Standard (AES) has won the contest which was held by US government in 1997[5]. Firstly in 1998, where fifteen candidate was further reduced to five in 2000, then as finalists for forthcoming standard five algorithms were selected, which is a slightly modification of Rijndeal. Fifteen candidates were accepted in 1998 and bases public comments the pool was reduced to five finalists in 1999. In October 2000, one of their five algorithms was selected as the forthcoming standard: a slightly modified version of the Rijndeal .Joan Damen and Vincent Rijmen are the two inventors from Belgian from whom name the Rijndeal is based. Rijndeal is block cipher i.e. it has a fixed number of bits in a block. Input block given to a certain size, usually 128, and produces equivalent output block of 128. A secret key is used as a second input in transformation. Where the cipher is being used deceives, the size of keys mostly 128,192 and256 bits keys are used. The block size is 128 bits and key size supported by AES is 128,192and 256 bits . The supported size and size of block of Rijndeal should be multiple of 32 and this is take 128 bits as minimum and maximum is taken 256[6][7].In AES, block cipher is iterated where the block size remained same and fixed i.e. 128 bits and key lengths is change. All transformation operates on states, these states are transitional results. The states consists rectangular array of bytes, where block size is 128 bit or 16 bytes and its size is 4x4.(in Rijndeal version whose block size varies keeps row size fixes as 4 but varies its columns size varies and the column size is always block size divided by 32).The block diagram of AES discussed in figure-3 and some operations also discussed.

Operations of AES [10] are applied on the state during each round are:

1. **Sub Byte:** In this round all bits are replaced by the other in state and this is done in Rijndeal S-Box

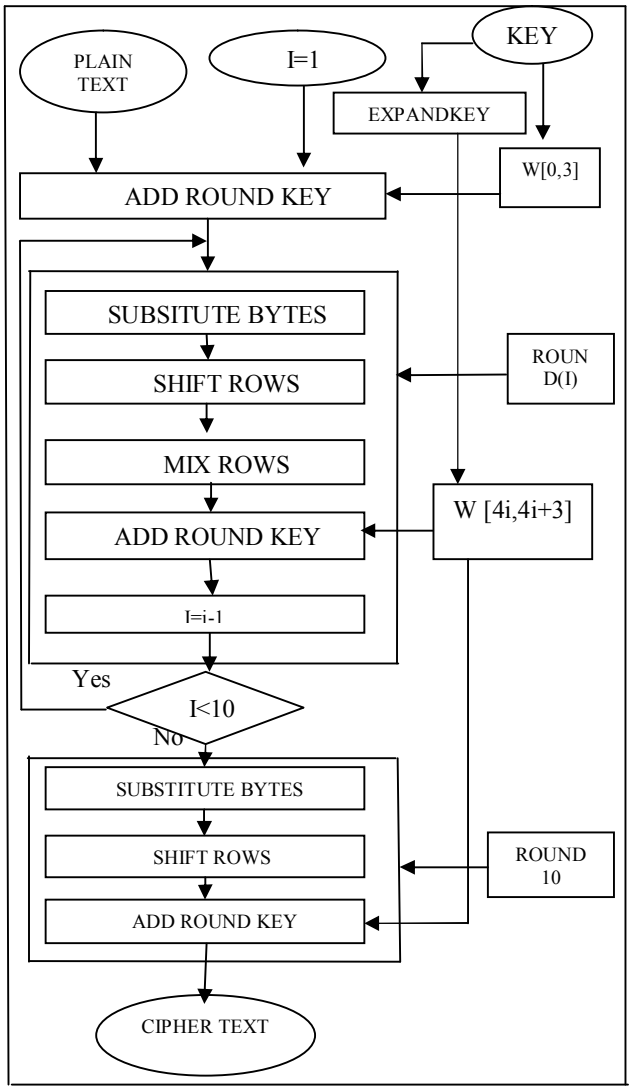

Figure-3 Block diagram of AES encryption

2. Shift Row: All rows are shifted to left by some amount the 4x4

3. Mix Column: Here the linear transformation is done on the columns of array.

4. Add Round Key: After the iterations, each byte of the state is joined with a round key, and that round key varies for each round and we originate that from the Rijndeal key schedule. Explain in the block diagram in Figure-3.

There are operations discussed above, perform sequentially to encrypt the data with the key and make the secure to improve the privacy of data.

III. EXPERIMENTAL DESIGN

We have discussed suppression techniques against unauthorized party. We used dual core Intel Pentium(R) of RAM 2GB and hard disc of 500 GB for this technique. Implementing AES and DES using MATLAB 7; on basis of one bit variation i.e. avalanche effect [8], memory used and time for simulation. We derived the performance of AES and DES in tabular form and in figures, given below.

IV. RESULTS AND ANALYSIS

The comparison of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) is shown below in the TABLE-I on the basis of avalanche effect.

TABLE-I

Technique	Keeping key constant 1 bit variation	Keeping plain text constant 1 bit variation
AES	83	81
DES	43	41

In AES, the avalanche effect is more than in DES. The one bit variation in DES, when we keep key constant is 43 while in AES, it is at 83 and similarly in AES, one bit variation in plain text constant is at 81 while in DES is at 41. The graphically result shows in figure-4 in the form of bar graph.

The comparison, on the basis of Memory usage for implementation of AES and DES, shows in TABLE-II, and also bar graph of memory required shows in Figure-5.

TABLE-II

Techniques	Simulation time	Memory required for implementation
AES	0.32	43.3
DES	0.0304	10.2

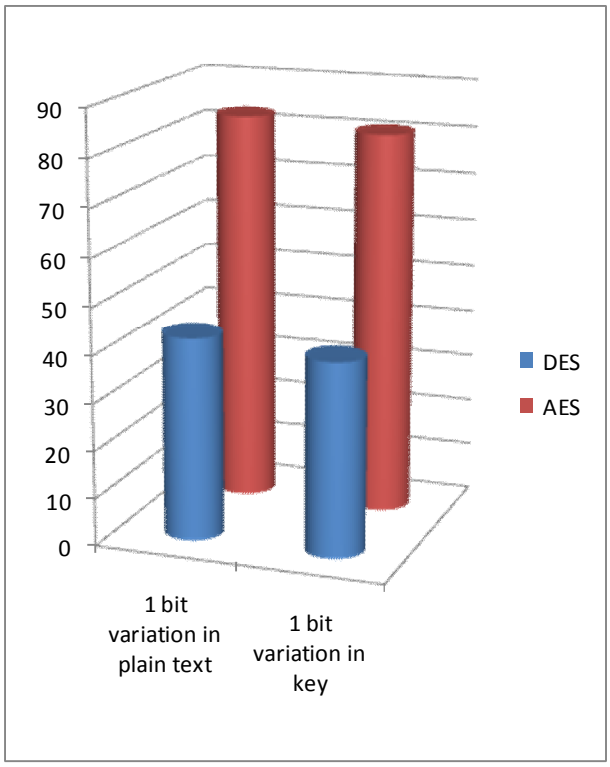

Figure-4 variation in plain text and key

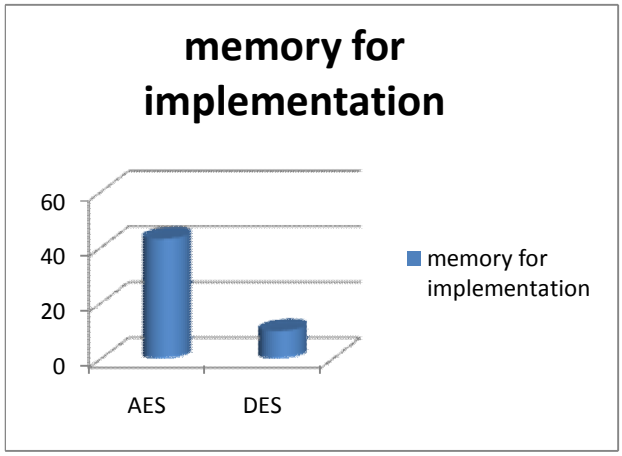

Figure-5 Memory implementation

In Figure-5, larger memory required for implementation in Advanced Encryption Standard (AES) as compare to Data Encryption Standard (DES) and in Figure-6; it is also clear that simulation time in AES is more effective as compared to DES.

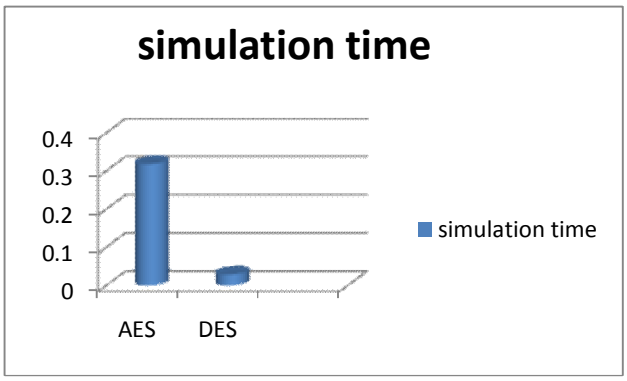

Figure-6 Simulation Time Result

V. CONCLUSION

Cryptography plays vital role in the security to maintain the confidentiality, authentication, integrity and non- repudiation of the information; and the encryption is the backbone of cryptography. The some significant issues in encryption have been discussed in this paper like simulation time, memory usage and One bit variation for performance estimation of DES and AES algorithms. The experimental results are shows in figures and in tabular form above on the basis of these issues. In financial application encryption in done by DES but Memory usage is DES is more than in AES .Avalanche effective i.e. One bit variation is more in Advanced Encryption Standard (AES) as compare to Data Encryption Standard (DES). AES is mostly used in encryption of message in chat Channel and is also used in monumentry transaction. AES provides the improvement in security level in information world as compared DES.

REFERNCES

[1] William Stalling "Cryptography and network security"Pearson education,2nd Edition

[2] Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader,Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms",international journal of network securit vol.10,No.3,pp,216-222,May 2010.

[3] Akash Kumar Mandal1, Chandra Parakash2 "Performance Evaluation of Cryptographic Algorithms: DES and AES", 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[4] Himani Agrawal and Monisha Sharma "Implementation and analysis of various symmetric cryptosystems " Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010)

[5] "Advanced Encryption Standard (AES)" Federal Information Processing Standards Publication 197, Nov. 26, 2001.

[6] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn

[7] R.Rivest, A. Shamir, L.Adleman."A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, Feb 1978.

[8] E. Kalai Kavitha "Performance Evaluation of Cryptographic Algorithms: AES and DES for Implementation of Secured Customer Relationship Management (CRM) System "IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 4 (Nov. - Dec. 2012), PP 01-07

[9] Aman Kumar , Dr. Sudesh Jakhar , Mr. Sunil Makkar "comparative analysis between DES and RSA algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[10] Bin Liu, and Bevan M. Baas, "Parallel AES Encryption Engines for Many-Core Processor Arrays," IEEE TRANSACTIONS ON COMPUTERS,2013, Digital Object Identifier no. 10.1109/TC.2011.251.