A Comparative Study of AES vs DES- A Review

Praveen Kumar[#1], Dr. Poonam Singhal[*2]
[#]*Department of Electronics and Communication, Deenbandhu Chhotu Ram University of Science and Technology*
[1]antilpk.pk@gmail.com
[2]singal.poonam@rediffmail.com

***Abstract*— In this modern world, the internet is the heart of the communication system. The Internet has revolutionized every sector of life. Now a days we share a lot of digital data through the internet, the main concern is security for personal and confidential data which is shared via the internet. The efficient way to secure digital data is by encrypting the data. Cryptography plays a crucial role in the transmission of data. In cryptography, we encode the data at the transmitter end and decode at the receiver end. Symmetrical encryption is the easiest way to encrypt and decrypt data. In this paper, studied the two most popular algorithms of encryption i.e AES and DES. These two algorithms are analyzed on various parameters, the ability to secure data, key size, etc.**

***Keywords*— AES, DES, Key Size, Block Size, Avalanche Effect**

I. INTRODUCTION

Information security is on the top priority for a national information and for personal data. To protect this digital data from a hacker while sharing through the internet we use cryptography process. There are two ways to protect data from hacking, first is by cryptography and second is by fragmenting data into small segments and sending it to the receiver via different paths. The problem with the second method is that we can't control data transmission path and if some packets are hacked then the hacker can predict remaining information from the packets he trapped. So, the only method we left with is cryptography. Cryptography is a process in which data is encrypted at the transmitter end and decrypted at the receiver end. There are two categories of cryptography (i) Symmetrical and (ii) Asymmetrical. In this paper, we focus on the symmetrical encryption process.

Symmetrical encryption is a process in which a single key is used to encode and decode the digital data. With the help of the key plain digital data is converted to cipher data. The main point of notice that, the same key is used for encryption and decryption. This process is also called secret key or private key process. The system which uses this type of communication actually exchanges key (private key) before actual communication starts[1].

Advantages of symmetrical encryption-

I. Fast Encryption.
II. Easy to implement.
III. Number of algorithms available i.e. AES, DES, 3DES etc.

Disadvantages of symmetrical encryption-

I. Key sharing in the network is the main issue. If the key is tapped by another node of the network than there is no benefit of encryption.
II. With the huge number of nodes in the network, key exchange increases. The complexity of the network is increased with an increase in a network node.

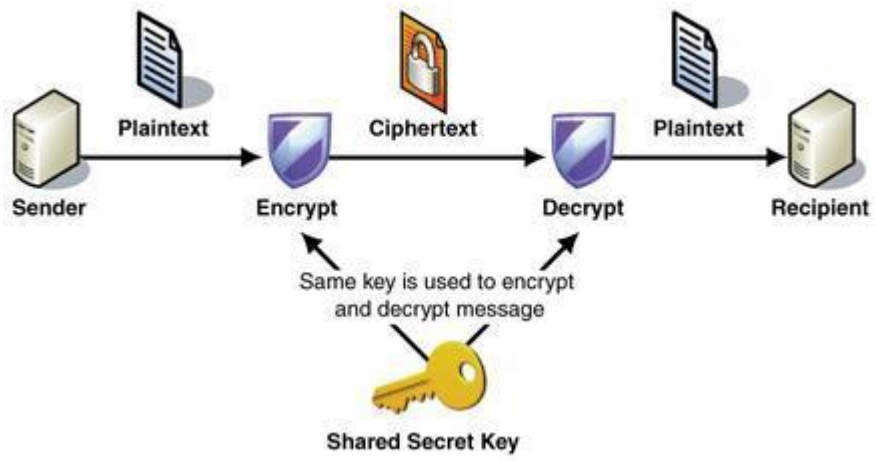


Fig. 1 Process of Symmetric Encryption [9]

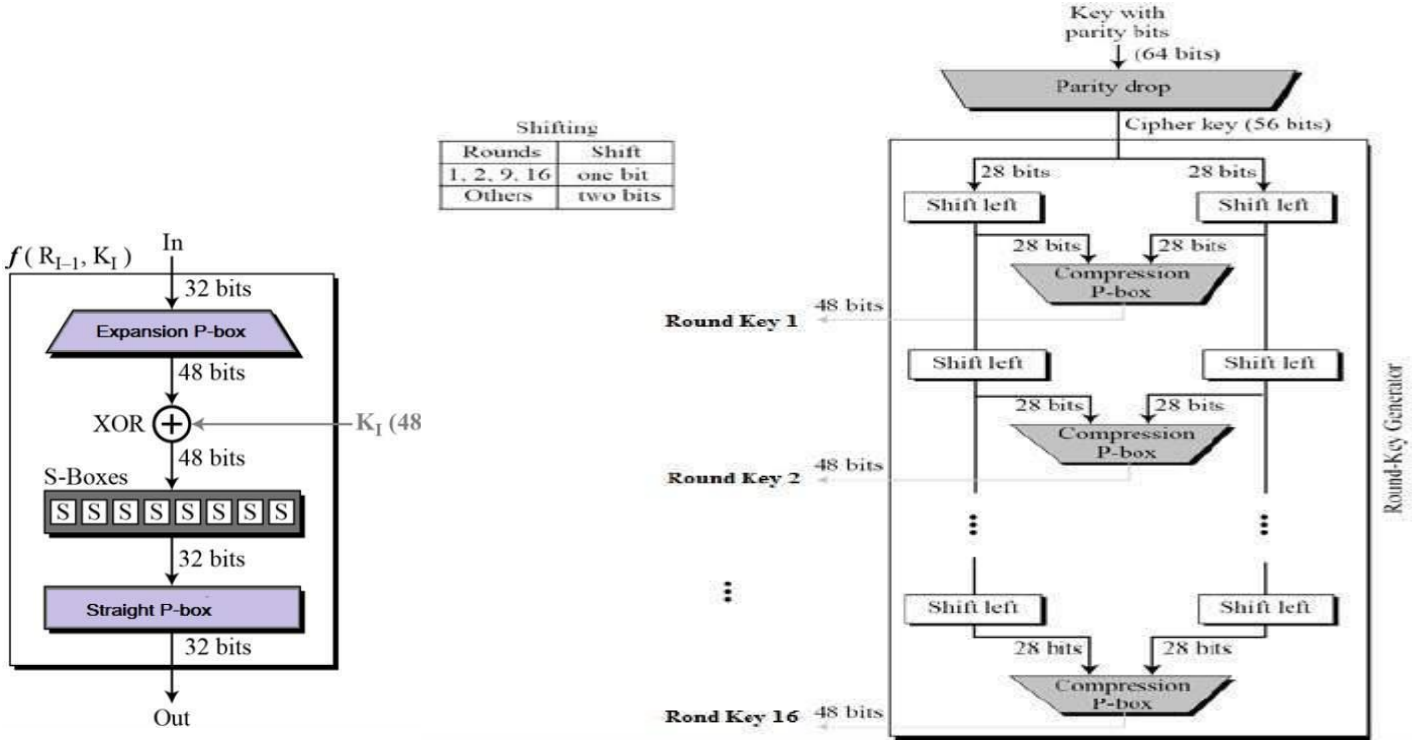
Due to its ease of implementation and a large number of available algorithms it is used in various applications. So, that's why this manuscript focuses on two of the most popular encryption algorithms i.e. AES and DES. Some important terms used in this paper are defined below-

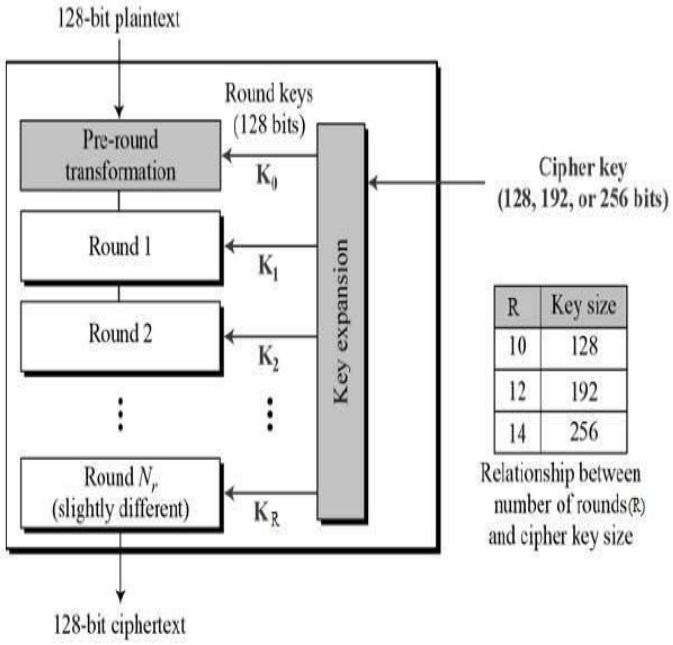
I. Plain Text/Data – This is the original data which is available at the sender end or transmitter side. This data can be read and understood very easily.
II. Cipher Text/Data – It is obtained after the encryption process is completed. This type of data can't be understood without decrypting.
III. Avalanche Effect – It is an important property of encryption algorithm, minute alteration in plain text/data results in a pronounced change in ciphertext/data[1].
IV. Completeness – This defines each bit of ciphertext depends on many bits of plain text.

II. DES Encryption Algorithms

DES is an acronym of Data Encryption Standard. It was first published by NIST (National Institute of Standard and Technology). DES is an example of the implementation of Feistel Cipher[2]. DES is a 16 round encryption Feistel structure. The block size on which DES operates 64- bits. The key length is of 64-bits, but all the bits are used not used out of 64-bits only 56-bits are used for the encryption process. Remaining 8-bits perform the function of check bits [3][4]. In DES, need to specify some functions- (i) Round function, (ii) Key schedule and (iii) Initial and Final permutation.

The round function is very important for DES function. DES applies 48-bits of the key to the 32-bits of the right most of the data to produce 32-bits of output. Round function comprises of Expansion P-Box, XOR, S-box, and Straight permutation. Expansion Permutation box is used to expand 32-bits into 48-bits. XOR operation is operated on the data generated by P-box with a round key. Substitution Box is used for mixing. DES employs 8 S-Boxes, which uses 48-bits as input and gives 32-bits as output. These 32-bits are now subjected to Straight Permutation[5][6].





R	Key size
10	128
12	192
14	256

Fig. 2 Round Function and Key Generation [12]

Key is generated by the round key originator which creates sixteen 48 bit keys out of 56-bit cipher key. Later an enhanced version of DES is introduced which is called 3DES or triple DES. In 3DES, single DES encryption process is applied on a particular data three times to encrypt it. And three-time decryption is done at the receiver end. This increases the strength of the encryption.

III. AES Encryption Algorithms

With the increase in data sizes, the encounter of the disadvantage of DES encryption process that it is a very time-consuming process. This due to the operation of DES on very block small size of data. So an alternative was introduced which is AES. AES stands for Advanced Encryption Standard. The main key feature of this encryption algorithms is that it operates on 128-bits of data and 128/192/256-bits of key length which increases the strength of encryption and AES can be implemented with the language C and Java[3][2]. It uses a combination of series which are linked with each other, some of them substitute and some perform permutation. AES operates on bytes rather than bits. That means 128 bits are considered as 16 Bytes of data. These 16 bytes are arranged in a matrix form. As, DES performs 16 round, AES performs variable rounds which depend on the key length used for encryption process[4].

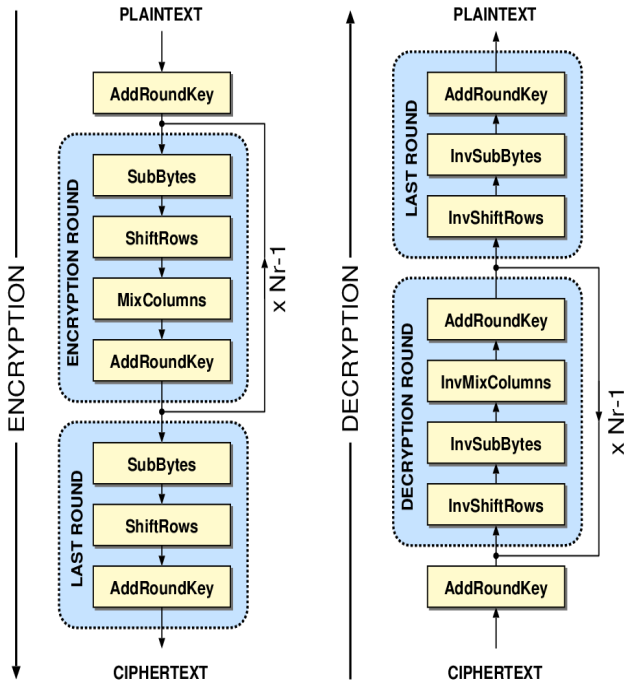


Fig. 3 AES Structure and Encryption Process [10][11]

Encryption process comprises of four subprocesses (i) Add Round key (ii) Substitution Byte (iii) Shift Row and (iv) Mix Columns. These four processes are used again for decryption but in reverse order. Add round performs XOR function on the 16 bytes by considering it as 128 bits with 128 bits of the round key[6]. In the last round, this process gives us the ciphertext. But for the intermediate process, it gives input to SubByte. The SubByte performs the action of substitution by looking into a fixed table maintained by S-Box. After that shifting operation is performed on the rows of the matrix (4*4 matrix). Then mixing of columns is done by special mathematical operations which replace the existing values of the matrix and give a completely new matrix. This operation is not performed in the last round[5][7].

AES used in various applications due to a number of reasons-

I. The security level of encryption is quite high.
II. Variable key length.
III. Due to implementation in C and Java it is flexible.
IV. Consumes less processing unit[8].

IV. Comparison of AES vs DES

TABLE I- AES vs DES

Parameter	DES	AES
Introduced Year	1974	1998
Developer	IBM	Vincent Rijmen and Joan Daemen
Length of Key	56 bits	128, 192 & 256 bits
Size of Block	56 bits	128 bits or 16 bytes
No. of Rounds	16	Depend on key length (10, 12 & 14)
Algorithm Structure	Feistel	Substitution- Permutation
Security	2^{56}	2^{128},2^{192} & 2^{256}
Flexible	Not Flexible	Flexible
Encryption Strength	Low	High
Enhanced Version	3DES	No Enhance Version
Usage of Processing Unit	Uses More Memory	Less Memory is Used
Power Consumption	High	Low
Speed	Slow	Fast

V. Conclusions

In this paper, we have studied the two most widely used encryption algorithms i.e. DES and AES. DES was a very old algorithm but still can be used for various applications. But AES is more superior to DES. The drawbacks of DES are positive points of AES. DES is used for a small block of data, key length is also fixed and very small, the encryption strength is also low and to use DES we require more processing power with high power consumption. But on the other hand we have, AES which is more secure, operates on a large block of data and the key block is also of various length this increases the encryption and strength of encryption. One of the major plus points is its requirement of low memory usage for encryption while consuming low power. As modern devices have high processing power but have limited power supply (for mobile devices). For this reason, AES best-suited encryption process for modern devices to protect digital data from the attacker.

References

[1] S. Kansal, “Performance Evaluation of Various Symmetric Encryption Algorithms,” pp. 105–109, 2014.

[2] A. Gupta and N. K. Walia, “Cryptography Algorithms : A Review,” vol. 2, no. 2, pp. 1667–1672, 2014.

[3] M. Usman *et al.*, “A Comprehensive Comparison of Symmetric Cryptographic Algorithms by Using Multiple Types of Parameters,” vol. 18, no. 12, pp. 131–137, 2018.

[4] M. Umair, “Comparison of Symmetric Block Encryption Algorithms Comparison of Symmetric Block Encryption Algorithms,” no. April, 2017.

[5] B. Bhat, A. W. Ali, and A. Gupta, “DES and AES performance evaluation,” *Int. Conf. Comput. Commun. Autom. ICCCA 2015*, pp. 887–890, 2015.

[6] G. Singh and S. Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security,” *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 33–38, 2013.

[7] A. K. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of cryptographic algorithms: DES and AES,” *2012 IEEE Students’ Conf. Electr. Electron. Comput. Sci. Innov. Humanit. SCEECS 2012*, pp. 1–5, 2012.

[8] J. Thakur and K. Nagesh, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 2, pp. 6–12, 2011.

[9] https://www.researchgate.net/figure/The-process-of-symmetric-encryption-2_fig1_260134733

[10] https://crypto.stackexchange.com/questions/2711/does-the-mixcolumns-step-come-before-or-after-addroundkey-in-aes-decryption

[11] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard

[12] https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm