Performance Evaluation of Various Symmetric Encryption Algorithms

Shaify Kansal
Centre for Computer Science and Technology
Central University of Punjab
Bathinda, India
shaifykansal@gmail.com

Meenakshi Mittal
Centre for Computer Science and Technology
Central University of Punjab
Bathinda, India

***Abstract* -With rise in the use of internet in various fields like banking, military and government sector, the security and privacy of the data has been the main concern. Today, most of the data handling and electronic transactions are done on the internet. When the information is transferred from the sender to the receiver over the internet, it may be eavesdropped by an intruder and thus is a continuous threat to the secrecy or confidentiality of the data. The popular technique that protects the confidentiality of the data is cryptography which converts the plain text into unreadable form and then receiver applies reverse mechanism to decrypt the unreadable form of data to readable form. This mechanism is called as encryption-decryption process. Thus to secure the data over the internet, it is important to find out which algorithm performs better than the other algorithms. In this paper, the different symmetric encryption algorithms like DES, 3DES, AES have been analyzed with respect to different parameters and data types (like text files, image) on i7 processor.**

Keywords—DES, 3DES, AES

I. INTRODUCTION

The internet today has greatly influenced the people around the world with the increased utility of the internet applications by the general population throughout the globe. Everyday a large amount of security related information is accessed and transferred across the internet in real-life applications. When the information is transferred from the sender to the receiver over the internet, it may be eavesdropped by an intruder and thus is a continuous threat to the secrecy or confidentiality of the data. The popular technique that protects the confidentiality of the data is cryptography. Cryptography as the word suggests is the combination of two words crypto (meaning secret or hidden) and graphy (an art of writing).Thus Cryptography can be stated as the art of writing which involves the transition of messages to a concealed form or unintelligible data. The data is unintelligible in the sense that understanding of the data is difficult or impossible. The terms encryption and decryption are mainly used with the cryptographic process. Encryption is the process involving the changeover of human-readable plain-text to the cryptic (cipher) text. Encryption has its reverse process known as decryption where cryptic text is converted back to the plain text or human-readable form [1]. In Fig. 1, the plain text is converted into the cipher text by applying the encryption procedure and the cipher text is converted back to the plain text through the process of decryption.

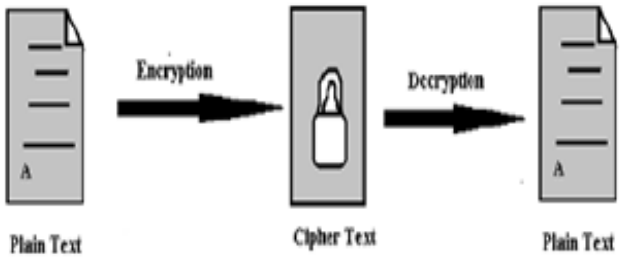

Fig. 1. Encryption-Decryption Flow

The Cryptographic process makes use of an algorithm and a secret (key) value. The key can be same for both encryption-decryption process or can be a different one depending on the type of encryption algorithm used. Depending upon the type of key used, cryptography techniques can be divided into two different categories - Symmetric (secret) and Asymmetric (public) key encryption.

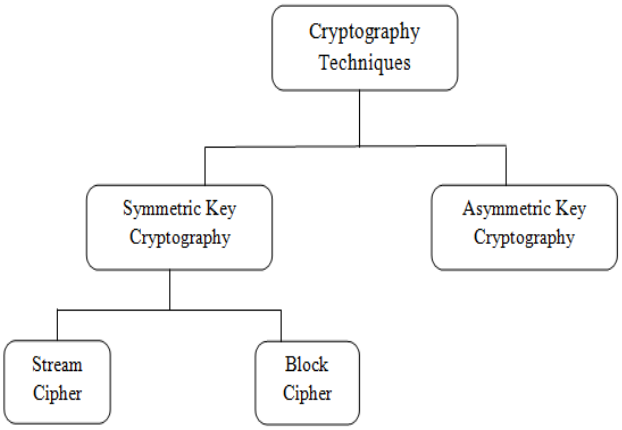

Fig. 2. Classification of cryptography techniques

Symmetric key encryption is the type of encryption method where the sender and receiver makes use of the same secret key for encryption as well as decryption process. Because a single key is used for both functions, secret key cryptography is also called symmetric key encryption. Examples of symmetric key encryption algorithms are DES, 3DES, AES, Blowfish [3].

In the **asymmetric key encryption**, two different keys (public and private keys) are used in encryption and decryption process. One key is used for encryption and the other one is used for decryption and vice-versa. The two keys are different but complementary in function. Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set and vice-versa. One such example of asymmetric cryptography is RSA algorithm [3].

II. ALGORITHMS IMPLEMENTED

A. Data Encryption Standard

As described in paper [9], DES was the first encryption algorithm to be published by NIST (National Institute of Standards and Technology). It was designed by IBM based on their Lucifer cipher. DES became a standard in 1974 .It is a widely used method of data encryption which uses the private key. DES applies a 56-bit key to each 64-bit block of data and maps 64 bit input block into a 64 bit output block. This process involves 16 rounds or operations and can run in several modes. The size of the key involved in DES encryption is actually 64 bit although the key size used is only 56 bits as the least significant bit of each byte is either used as a parity bit. DES was considered as an insecure block cipher due to its vulnerability to the brute-force attack and relatively small key-size.

B. Triple Data Encryption Standard

Triple Des was developed as an alternative to address the flaws in DES without designing a new cryptosystem. 3DES preserves the existing investment in software and equipment by using multiple encryptions with DES and multiple keys. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. It uses as input 64-bit plaintext to produce 64-bit cipher text, similar to DES. But unlike DES the combined key size is thus 192 bits with actually key-size usage of 168 bits (3 times 56).3DES is thus slower than other block cipher method as it essentially applies the DES algorithm three times. In this paper, two keys are used for 3DES encryption (K1,K2, K1) describing encrypt(k1)-decrypt(k2)-encrypt(k1) mode and for decryption decrypt(k1)-encrypt(k2)-decrypt(k1) mode [9].

C. Advanced Encryption Standard

The two major problems faced by the earlier algorithms were the small key size (in case of DES algorithm) and slow speed (Triple des algorithm). To overcome these shortcomings; NIST (National Institute of Standards and Technology) published a new encryption algorithm known as AES (Advanced Encryption Standard) in 2001. AES is an important symmetric block cipher that has replaced DES for the wide range of applications .The AES encryption algorithm is a block cipher as it works on a single block of data at a time. AES makes use of an encryption key and several rounds of encryption [10]. The AES takes as input the block length of 128 bits and the key length of 128,192 or 256 bits corresponding to 10, 12 or 14 rounds.

III. EXPERIMENTAL SETUP

In order to compare the performance of various algorithms, the simulation is done in C language, compiled with Borland C++ Compiler. Table I describes the simulation scenario followed.

TABLE I. SIMULATION SCENARIO

Different Algorithms	**Performance Metrics**	**Different Data**	**Hardware Configuration**
DES	Encryption-Decryption Time, Throughput, Memory Utilization	Text Files (15KB, 70KB, 2MB) Image file	Intel(R)Core (TM) i7-3700 CPU
3DES			
AES			

The various performance metrics [6] that are evaluated include–

Encryption Time - The encryption time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. It is measured in seconds.

Decryption Time - The decryption time is the time that a decryption algorithm takes to produce a plaintext from a cipher text. It is measured in seconds.

Throughput - The throughput of an encryption or decryption scheme defines the speed of encryption. The throughput of the encryption can be calculated as in equation –

$$\text{Throughput} = \frac{\text{Tp (Kilobytes)}}{\text{Et (Second)}}$$

where Tp: Total plain text (Kilobytes)

Et: Encryption time (second)

Memory Utilization - The Memory Utilization defines how much memory is being consumed by the process while doing encryption or decryption. It is measured in Kilobytes (KB).

A. Encryption and decryption of text files

The results for the text files are shown as below--

Experiment – Calculation of encryption time, decryption time, throughput, memory utilization for text files of different size.

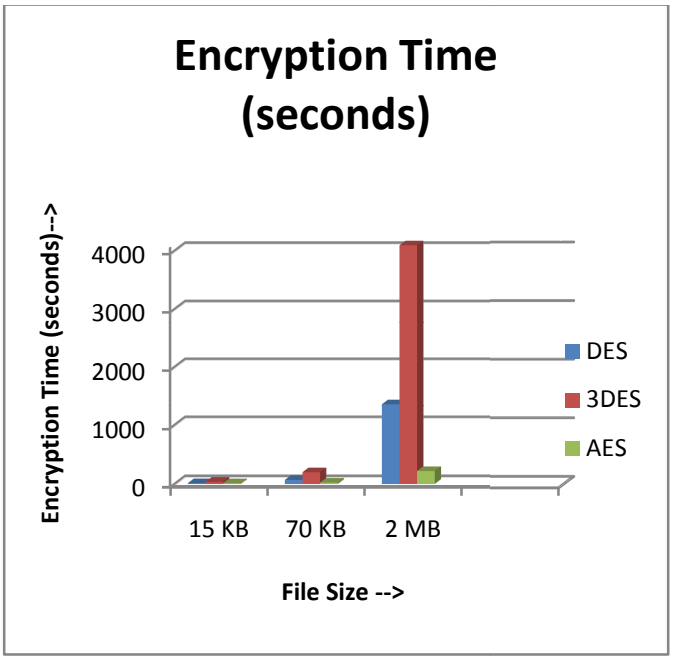

Fig. 3. Comparison of Encryption Time for various algorithms

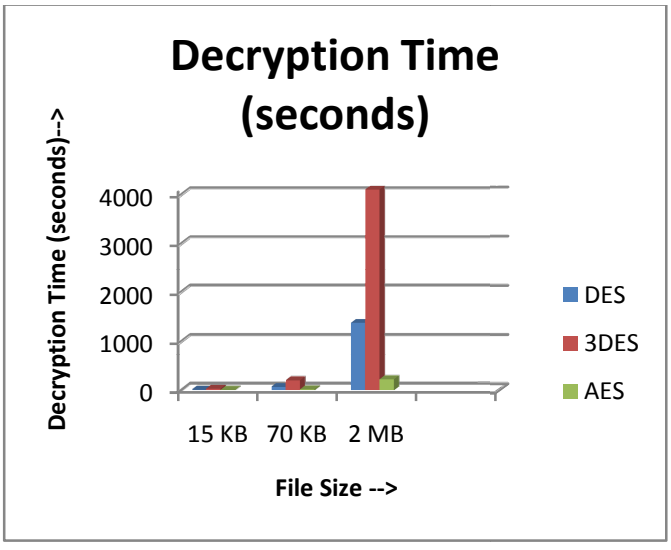

Fig. 4. Comparison of Decryption Time for various algorithms

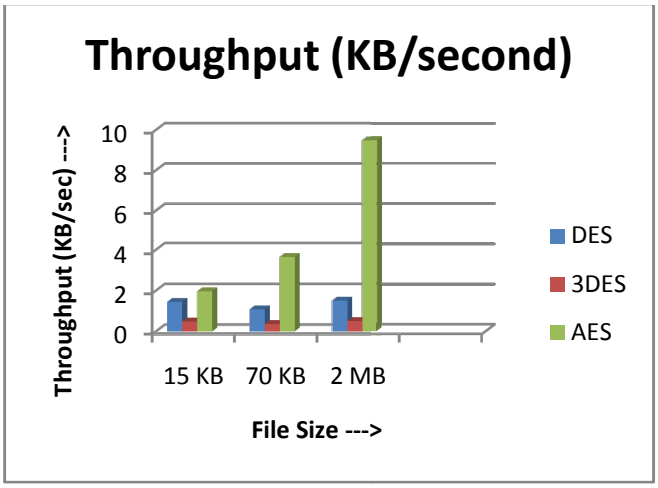

Fig. 5. Comparison of Throughput for various algorithms

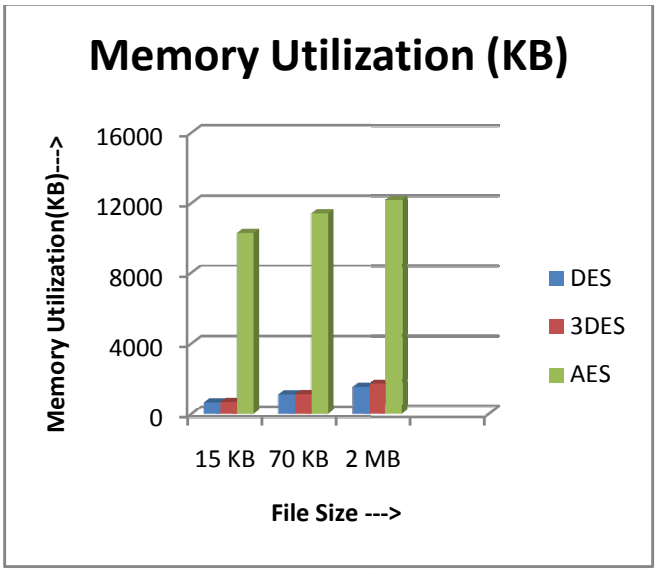

Fig. 6. Comparison of Memory Utilization for various algorithms

Analysis – It has been analyzed that for text files of different sizes, AES algorithm takes less encryption and decryption time compared to other algorithms. Throughput varies inversely to the encryption or decryption time. Thus it is more in case of AES algorithm. Memory utilization of DES is less than the other algorithms.

B. Encryption and decryption of image

The image encrypted is shown in Fig. 7

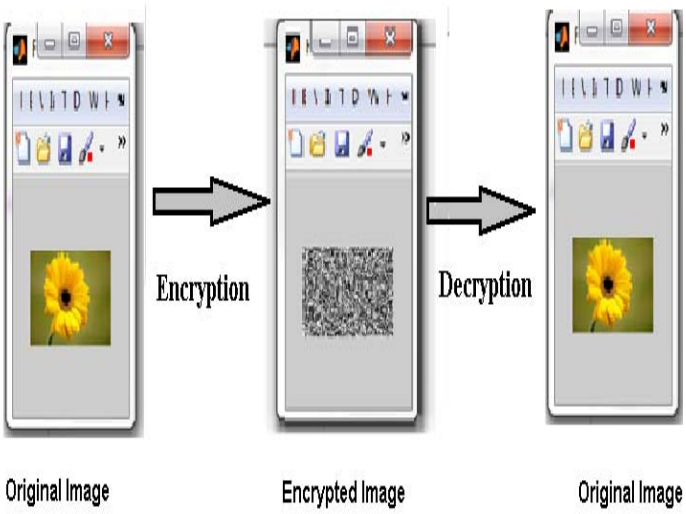

Fig. 7. Original and Encrypted Images

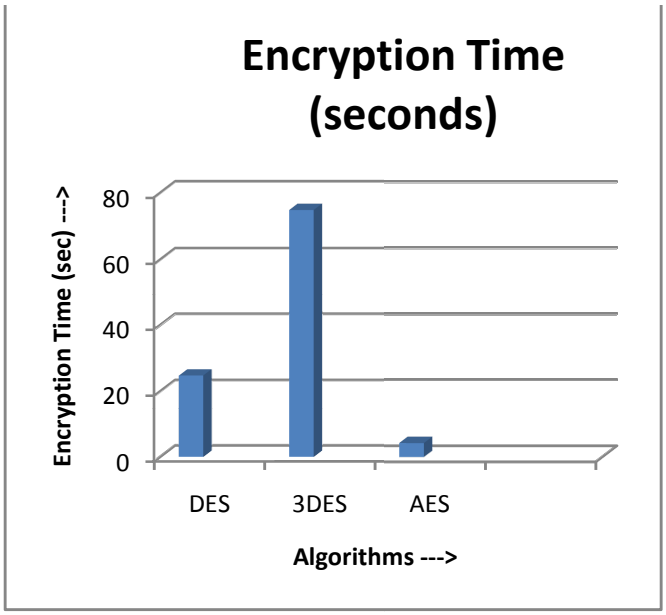

Fig. 8. Comparison of Encryption Time for various algorithms

Experiment – Calculation of encryption time, decryption time, throughput, memory utilization for image.

Results – Results collected are shown in Table II.

TABLE II. COMPARISON OF DIFFERENT ALGORITHMS FOR IMAGE DATA TYPE

IMAGE	DES	3DES	AES
ENCRYPTION TIME (SECONDS)	24.571	74.716	4.143
DECRYPTION TIME (SECONDS)	24.571	74.716	4.413
THROUGHPUT (KB/SEC)	0.244	0.0803	1.448
MEMORY UTILIZATION (KB)	610	690	10016

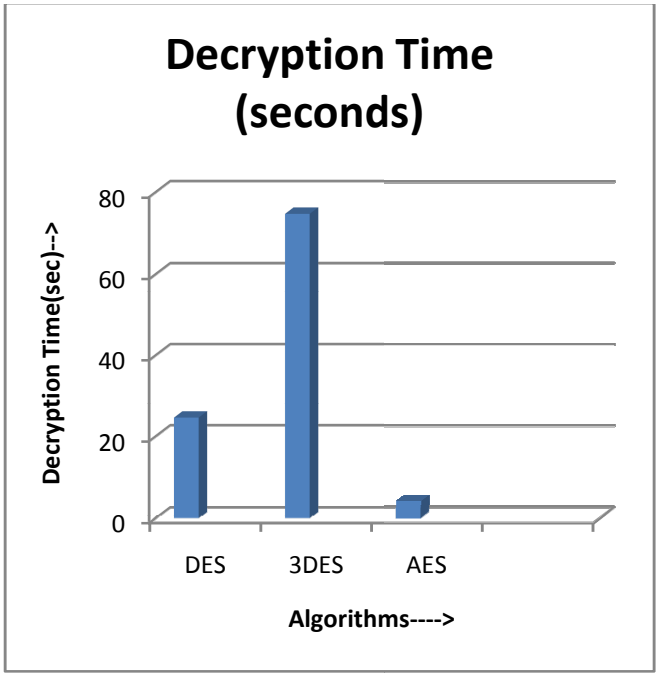

Fig. 9. Comparison of Decryption Time for various algorithms

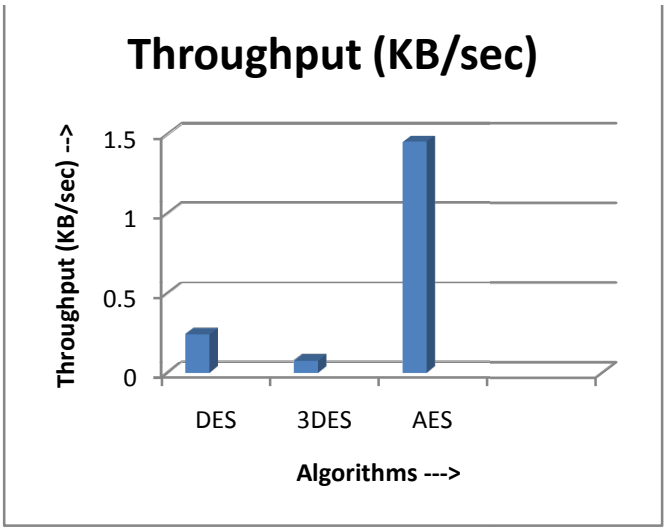

Fig. 10. Comparison of Throughput for various algorithms

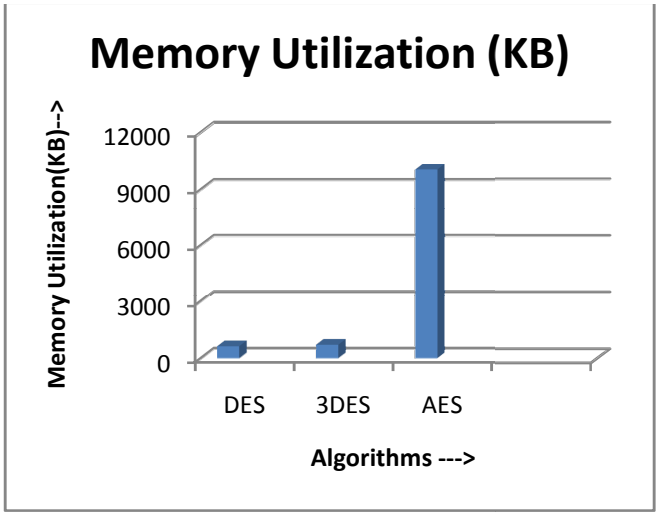

Fig. 11. Comparison of Memory Utilization for various algorithms

Analysis – It has been observed that for image data type, AES algorithm takes least time for encryption and decryption than the other algorithms. Throughput varies inversely to the encryption time. Thus it is more in case of AES and less in case of 3DES algorithm. Memory utilization of DES algorithm is less compared to other algorithms.

CONCLUSION

The paper presents the performance evaluation of different symmetric key encryption algorithms- DES, 3DES and AES for text and image data type.

The results show that encryption and decryption time of AES algorithm is less than other algorithms as the number of rounds is comparatively less in case of AES while 3DES has more encryption-decryption time as it applies the algorithm three times. Throughput varies inversely to the encryption or decryption time. Therefore, AES has more and 3DES has less throughput than the other algorithms. AES takes more memory while DES utilizes less memory than the other symmetric key encryption algorithms. In future, these encryption algorithms can be analyzed for audio and video data types.

REFERENCES

[1] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in *Information and communication technologies, 2005. ICICT 2005. First international conference on*, 2005, pp. 84-89.

[2] S. William and W. Stallings, *Cryptography and Network Security, 4/E*: Pearson Education India, 2006.

[3] O. Verma, R. Agarwal, D. Dafouti, and S. Tyagi, "Peformance analysis of data encryption algorithms," in *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 2011, pp. 399-403.

[4] D. S. A. Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," *IJ Network Security,* vol. 10, pp. 216-222, 2010.

[5] A. Tamimi, "Performance analysis of data encryption algorithms," *Retrieved October,* vol. 1, 2008.

[6] D. S. A. Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types," *IJ Network Security,* vol. 11, pp. 78-87, 2010.

[7] N. Penchalaiah and R. Seshadri, "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)," *International Journal of Computer Science and Engineering,* vol. 2, pp. 1641-1645, 2010.

[8] N. Singhal and J. Raina, "Comparative analysis of AES and RC4 algorithms for better utilization," *International Journal of Computer Trends and Technology,* vol. 79, pp. 177-181, 2011.

[9] S. M. Seth and R. Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication 1," 2011.

[10] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," in *Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on*, 2012, pp. 1-5.