Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security

Gurpreet Singh, Supriya Kinger

Abstract—With the progression of digital data exchange in electronic way, information security is becoming more essential in data storage and transmission. Encryption algorithms play a major role in the information security systems. The main objective of the use of encryption algorithms is to protect data and information in order to achieve privacy. This paper provides the evaluation of encryption algorithms like AES, DES and 3DES. A comparison has been conducted for these encryption algorithms and AES is found to be the best encryption algorithm in terms of speed and security. This paper also proposes a new method to technique to encrypt files. AES, DES, 3DES algorithms have been used in parallel and results obtained are places together in a common file. Reverse process has been done to decrypt the encrypted file to obtain original text file.

Index Terms— Information Security, Cryptography, Encryption Algorithm, AES, DES, 3DES, Encryption, Decryption.

1 Introduction

With the speedy development of computer technology and advancement of internet, the importance and value of exchanged data are increasing. The widen usage of digital media for information transmission through secure and unsecured channels exposes messages sent via networks to intruders or third parties. Therefore to counterpart this weakness, many researchers have come up with efficient algorithms to encrypt information from plain text (or clear text) into cipher text (or encrypted data) [1].

Cryptography is a key technology for achieving information security in various fields such as computer science, e-commerce, and in the emerging information society. Cryptography is the art of combining some input data, called the plaintext, with a user-specified password (or key) to generate an encrypted output, called cipher text, in such a way that, given the cipher text, it is extremely difficult to recover the original plaintext without the key. A key is a sequence of symbols that controls the cryptographic operations, such as encryption, decryption, signature generation or signature verification [2], [3]. The simplicity or complexity of encryption process depends on encryption algorithm and the key which is used in algorithm to encrypt or decrypt the data. According to the Kirchhoff, the security of the encryption system should depend on the secrecy of the key rather than encryption algorithm. The security level of the encryption algorithm should depend on the size of the key space, secrecy of the key, length of the key, initialization vector and how they all work together.

Depending upon the number of keys used, modern cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). In symmetric algorithms, both parties (i.e. sender and receiver) share the same key for encryption and decryption whereas in Asymmetric algorithms two keys are used. One key is used for encryption, called "public key" and the other key is used for decryption, called "private key". Many schemes used for encryption constitute the area of study known as cryptography as shown in Fig. 1.

- *M.Tech Research Scholar, Dept. of CSE, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India. E-mail: gurpreet.s.saggu@gmail.com*
- *Assistant Professor, Dept. of CSE, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India. E-mail: supriya@sggswu.org*

2 Existing Encryption Algorithms

2.1 Data Encryption Standard (DES)

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key [4], [5].

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications [6], [7].

The flow of DES Encryption algorithm is shown in Fig. 2. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).

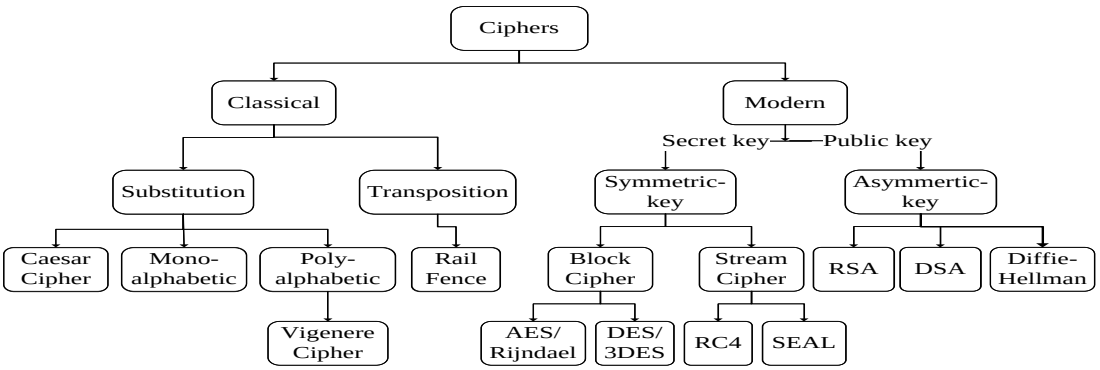

Fig. 1. Classification of Encryption Methods

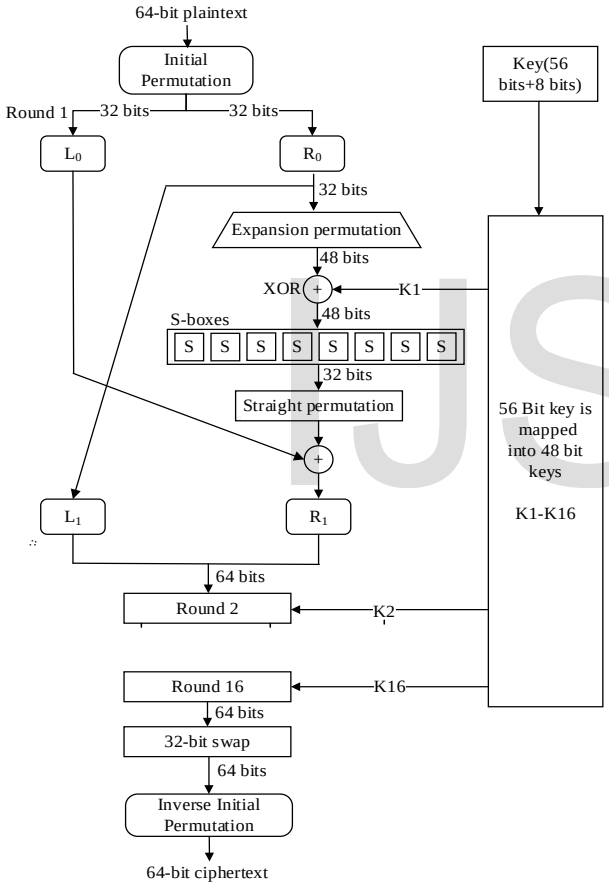

Fig. 2. General Depiction of DES [8]

2.2 Triple DES (3DES)

3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3 [9]. The standards define three keying options:

Option 1, the preferred option, employs three mutually independent keys (K1 ≠ K2 ≠ K3 ≠ K1). It gives keyspace of 3 × 56 = 168 bits.

Option 2 employs two mutually independent keys and a third key that is the same as the first key (K1 ≠ K2 and K3 = K1). This gives keyspace of 2 × 56= 112 bits.

Option 3 is a key bundle of three identical keys (K1 = K2 = K3). This option is equivalent to DES Algorithm.

In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [10], [11].

2.3 Advanced Encryption Standard (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text [12]. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation [6], [13]. Fig. 3 shows the overall process. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

Each round of AES is governed by the following transformations [4]:

1. Substitute Byte transformation

AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte

(8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael Sbox.

2. Shift Rows transformation

It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, is cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

3. Mixcolumns transformation

This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

4. Addroundkey transformation

It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

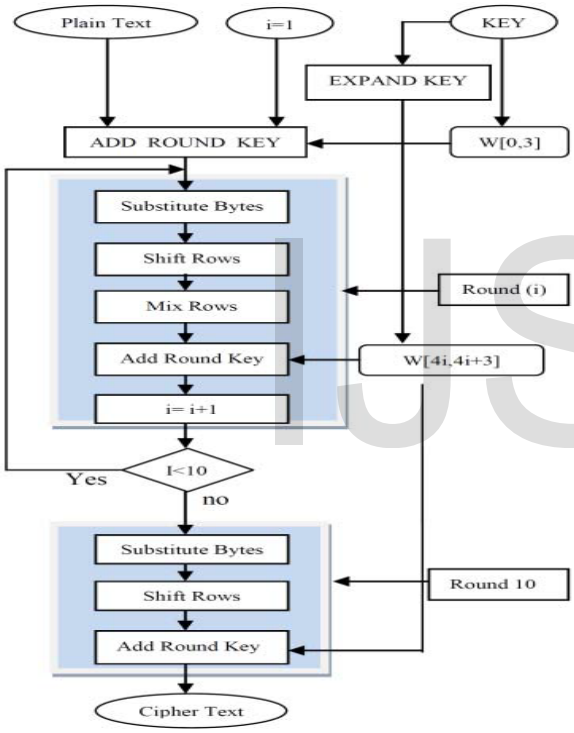

Fig. 3. AES (Advanced Encryption Standard) Process [4]

3 Proposed Work and Experimental Evaluation

In proposed work, the most popular modern encryption algorithms such as AES, DES and 3DES are stated. DES was one of the first encryption schemes used for electronic communications. Because it was found to be too weak, 3DES was created, which uses DES three times. But 3DES algorithm is not more popular primarily due to speed and out of these algorithms AES is better in terms of speed and security. AES is much harder to break than other two algorithms. Comparison of these three algorithms in terms of speed is shown in Fig. 4 and Fig. 5.

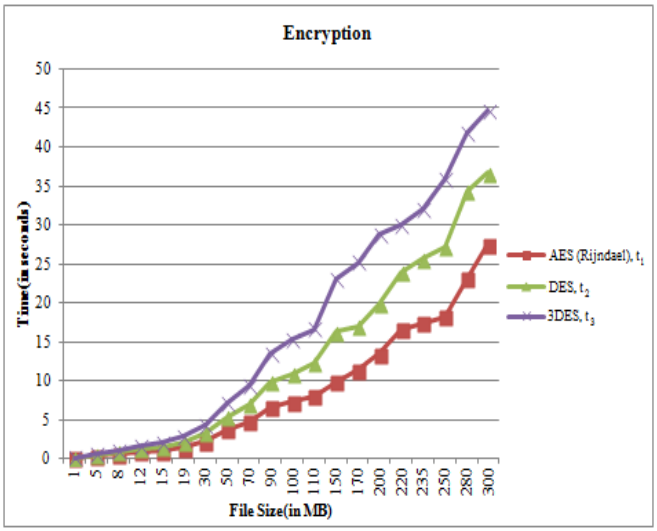

Fig. 4. Time taken by AES, DES and 3DES to encrypt file

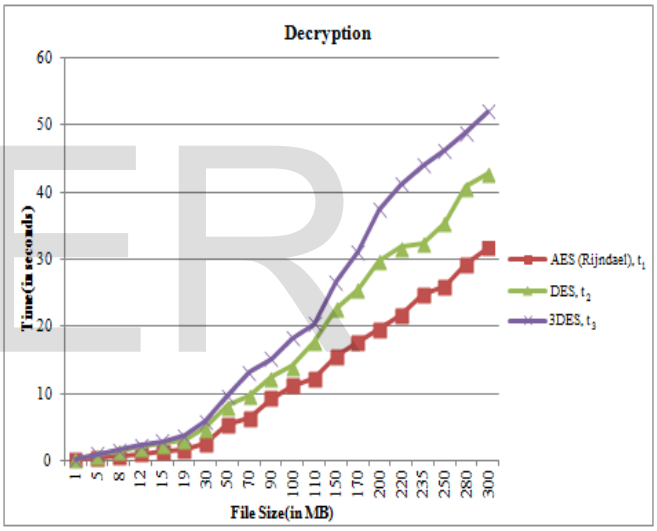

Fig. 5. Time taken by AES, DES and 3DES to decrypt file

In Fig. 4 and Fig. 5, AES, DES and 3DES algorithms have been compared w.r.t. time and file size. Here, t1 is the time taken by AES, t2 by DES and t3 by 3DES. X-axis shows the file size of text files selected randomly in MB and Y-axis shows the execution time in seconds. Fig. 4 shows the time to encrypt the data corresponding to file size whereas the Fig. 5 shows the decryption time. In both the processes, AES algorithm takes the least time as compared to DES and 3DES.

Fig. 6 shows the total time taken to encrypt the file using three algorithms (t1+ t2+ t3 is the total time taken) and also the time taken when the process of encrypting the file using three algorithms run in parallel. Fig. 7 shows the total time taken to decrypt the file using three algorithms and also the time taken when the process of decrypting the file using three algorithms runs in parallel. Clearly, it can be seen that time taken by all three algorithms running in parallel is less.

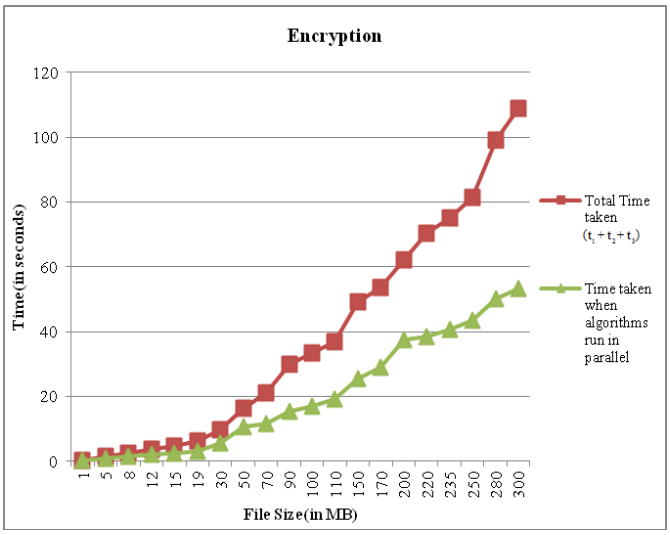

Fig. 6. Comparison between total time and time when algorithms run in parallel (Encryption)

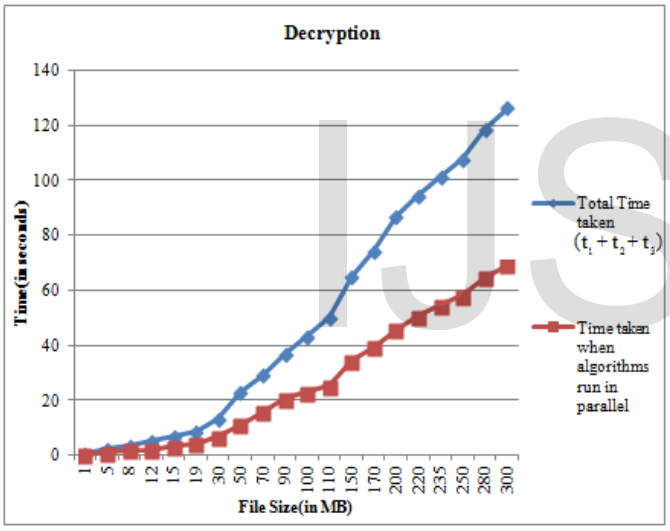

Fig. 7. Comparison between total time and time when algorithms run in parallel (Decryption)

In proposed work, first the input file is encrypted by using three algorithms AES, DES and 3DES then the result after encryption is merged into a single file using splitter "~ >6". The splitter is used to distinguish the result of three algorithms. Also, it helps to decrypt the merged file into three different files by using corresponding algorithms to get the input text. The file size of the merged file after encryption is three times (including size of splitter) than that of individual encrypted files generated by these three algorithms.

The advantage of above mentioned process is that the merged file is difficult to decrypt as three algorithms are being used instead of single algorithm. The intruder (or cracker) will not be able to predict which algorithm is being used in this process.

On completion of the whole process, the output files after decryption are compared with each other by using MD5 hashing algorithm to check if contents within the files are same.

3.1 Experimental Evaluation

The proposed work is applied to the file which contains the text "Information Security" and the steps to obtain the results for encryption are as follows:

Step- 1: Using the DES algorithm convert string "Information Security" into " 'M)ø(z=Óm7ÑëÓùhžð–Ÿ" by applying the 64-bit key K= {?, ", 1, ~, f, S, J, o}.

Step-2: Add the splitter "~ >6" to the output obtained in Step- 1. So the result becomes " 'M)ø(z=Óm7ÑëÓùhžð– Ÿ~ >6".

Step-3: Now, using 3DES algorithm convert string "Information Security" to get the encrypted string "0ç•=Š.£¹!‡™l=ZÜêIoÛ-{È" by using 192 bit key, K={ &, !, +, t, (, w, 5, {, s, j, H, -, 6, d, e, o, $, 2, 6, 1, <, a, @, #}.

Step-4: Add the output of 3DES algorithm to the result obtained in Step- 2. So the result becomes " 'M)ø(z=Óm7ÑëÓùhžð–Ÿ~ >60ç•=Š.£¹!‡™l=ZÜêIoÛ-{È".

Step-5: Again, add the splitter "~ >6" to the result obtained in Step- 4. It gives the result " 'M)ø(z=Óm7ÑëÓùhžð–Ÿ~ >60ç•=Š.£¹!‡™l=ZÜêIoÛ-{È~ >6".

Step-6: Finally, AES encryption algorithm having 128- bit key, K= {d, *, U, ?, ~, !, `, k, -, 2, f, a, [, l, t, k} is applied to the input string "Information Security" to obtain the result "ŒÃgÜ‡YF†¬t1o =‰ì=/Œ½ Q©Fy÷ò".

Step-7: The result obtained in the Step- 6 is added to the result obtained in Step- 5 to get the final result, which is " 'M)ø(z=Óm7ÑëÓùhžð–Ÿ~ >60ç•=Š.£¹!‡™l=ZÜêIoÛ-{È~ >6ŒÃgÜ‡YF†¬t1o =‰ì=/Œ½ Q©Fy÷ò".

The merged file contains the above final result. By applying the process of decryption the user will get the original text viz. "Information Security". Results shown above are for a text file containing small data "Information Security". Proposed work can also be applied to a file that contains huge data.

4 Conclusion and Scope of Future Work

In this paper, study of the three popular modern encryption algorithms has been done: AES, DES and 3DES. Modern Encryption Algorithms such as AES, DES and 3DES have been compared in this paper. Results show that AES algorithm takes less time to encrypt and decrypt the file as compared to DES and 3DES. Also, when the encryption algorithms are applied parallel to the same file then time taken to produce output file is less. Though, application of multiple algorithms increases time and space complexity of the system, but security of the system has become manifolds. Future research work can concentrate on including some more encryption algorithms along with compression techniques

to reduce memory requirements.

REFERENCES

[1] O P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, "Performance Analysis of Data Encryption Algorithms", 3rd International Conference on Electronics Computer Technology (ICECT) (Volume: 5), pp. 399 - 403, 8-10 April 2011.

[2] "Introduction", http://kremlinencrypt.com/concepts.htm

[3] IEC 18033-1, Information technology – Security techniques – Encryption algorithms – Part 1: General.

[4] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[5] Sriram Ramanujam and Marimuthu Karuppiah, "Designing an algorithm with high Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, pp. 106-111, January 2011.

[6] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[7] "DES", http://www.tropsoft.com/strongenc/des.htm

[8] Gurpreet Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, Volume 67– No.19, pp. 33-38, April 2013.

[9] "3DES", http://www.cryptosys.net/3des.html

[10] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[11] "3DES", http://en.wikipedia.org/wiki/Triple_DES

[12] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[13] Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, "AES and Confidentiality from the Inside Out", the 12th International Conference on Advanced Communication Technology (ICACT), pp. 1587-1591, 2010.