Optimized Approach for Secure Communication Using DES Algorithm

Gaurav Bothra, Chaitali Pandya and Animisha Parmar

***Abstract*—**Security remains a major "pain" for both individuals and large organizations in today's modern world. Everything needs security, whether it is communication through telephonic media, or transfer of data files. The security or privacy can only be ensured by applying algorithms to the data defined under Cryptography. Encryption, a mechanism which changes the plaintext to a secured form defined as scrambled text(cipher). The scrambled text, then is received and decryption is done to analyze the plaintext. This involves various types such as: symmetric or asymmetric encryption. This paper brings in an improved and optimized version of 3DES algorithm. It also lists various advantages of the new algorithm over DES and Triple-DES algorithm. A brief in between DES, Triple-DES and the newly designed algorithm (Optimized DES Algorithm) is provided taking amount of complexity, user effort required, key size and number of rounds to perform successful conversion operations as base for comparison.

***Keywords*—** Cryptanalysis, Cryptography, DES Algorithm, ODES, Security, Transmission.

I. INTRODUCTION

The challenge for security of data has increased nowadays. The content needs to be more secure, private for safe communications. The challenge mostly came into picture because of the open world, where everything is online and can be accessed through one or the other mediums. The insiders of the organizations are required to be given more attention than outsiders. Because, the insiders easily know where the data is stored, and is easy to access as these are stored in plain text format locally.

Cryptography is the exercise of certain techniques and algorithms which needs to be applied for safe communication when third party other than the communicating parties known as adversaries is present. The various aspects such as authentication, confidentiality, data integration are the pillars of modern cryptography. Mainly, Cryptography states two techniques: "Symmetric Cryptography" and "Asymmetric Cryptography" [1].

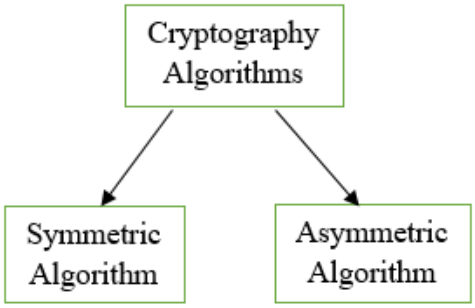

Fig. 1: Cryptography Algorithms

The symmetric cryptography requires the same/single key to be used for encryption/decryption. The source(sender) takes the key with an encryption technique to scramble the normal text. The destination uses that single key used by the source with a decryption algorithm to decrypt the text being scrambled by the source.

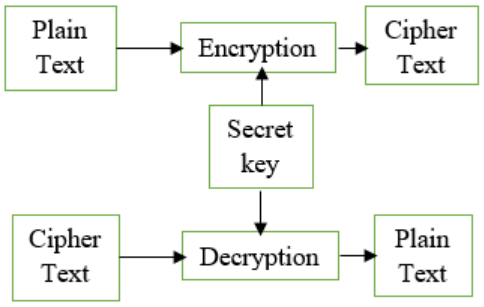

Fig. 2: Symmetric Cryptography Algorithm

Widely used Symmetric Cryptography alorithms:

- DES
- Triple DES
- AES

The asymmetric cryptography requires two different keys for encryption/decryption: public key and private key. The message is encrypted by the source using the general public key whereas private key is used to decrypt the message by receiver.

Gaurav Bothra, VIT University, INDIA,
E-mail:gauravbothra2017@outlook.com
Chaitali Pandya, VIT University,INDIA,
E-mail: chaitali.pandya2016@vitstudent.ac.in
Animisha Parmar, VIT University, INDIA
E-mail: animisha.parmar2016@vitstudent.ac.in

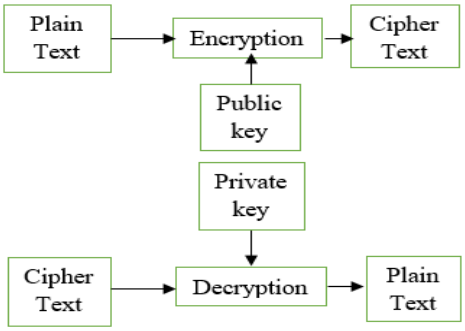

Fig. 3: Asymmetric Cryptography Algorithm

The most used Asymmetric Cryptography algorithms:

- RSA(Rivest-Shamir-Adlemen)
- Diffie-Hellman

There are various algorithms under cryptography such as: Secret Key, Public Key and Hash functions cryptography.

II. DATA ENCRYPTION STANDARD (DES)

The DES algorithm is an archetypal block cipher- taking the data input as a fixed length of plaintext and through applying various operations converts it into cipher text. It also involves a key to make transformation from original to scrambled text. So that, the process of changing back to normal form can only be done who knows about the key which was used in the process of encryption. The key in DES Algorithm consists of 64bits. But then, only 56bits are used in actual. The leftover 8bits are then used for checking parity, and are discarded. Hence, the used key length by the algorithm is 56bits [2].

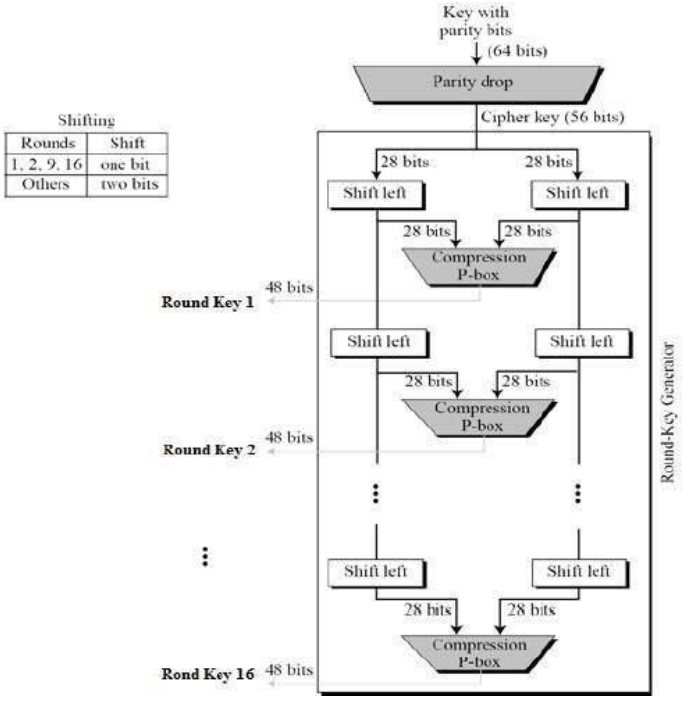

Fig. 4: DES Algorithm

This paper proposes new method to implement the DES Algorithm which is a way much secure than the DES Algorithm, but at the same time is faster than the 3DES. The proposed algorithm is termed as ODES algorithm (Optimized DES algorithm).

III. TRIPLE-DES ALGORITHM

In simple words, Triple-DES refers to three times of DES algorithm. The DES algorithm was successful in its way but then the increasing computational power lead it to be headed by brute force attacks. 3DES has a way to increase the length of the key to 168bits i.e. 56*3bits. It takes three 56bit keys (K1, K2, K3). Then, encrypting by k1 further by K2 and the last by K3. The 3DES is available in two versions: a) two-key version b) three-key version. In two-key version of the algorithm, the same algorithm is being implemented but K1 is being used for the first and the last encryption.

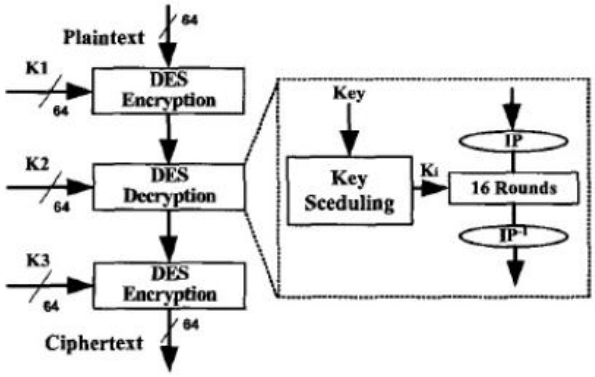

Fig. 5: Triple-DES Algorithm

IV. RELATED WORK

Many solutions have been mentioned regarding DES algorithm in the field of security and Cryptography. But for any block cipher algorithm, the most basic attack: Brute force. It is only possible because the length of key used in Single DES algorithm was only 56 bits removing 8 bits used for parity which was very small. Therefore, the possible number of keys to be determined was very easy. Then, after single DES algorithm the 3DES algorithm came into being. The Triple-DES used two 56bit keys as which provided the maximal security level is 112bit. And, with Meet-in-Middle attack the cipher could be divided into two separate halves which could be attacked easily by the intruder. The new ODES algorithm provides security as the encryption is done N times and only a main key used number of times which makes it difficult for the attacker or intruder to break or crack the algorithm.

V. THE ODES ALGORITHM

A. Key Generation Process

The new algorithm ODES provide more security as compared to the DES and 3DES Algorithm. As, the code makes the encryption process to happen more than 3 times, which

was fixed in the previous algorithms. Likewise, in DES algorithm it was fixed that user needs to enter a fixed length plaintext and also the same for key. But, this algorithm brings it to be variable i.e. the key and plaintext can be of any size entered by the user. Another advantage of this ODES algorithm is that only key is used to perform the number of time the encryption process whereas in Triple-DES it was required to enter three different keys to make the encryption successful.

The process how it works is explained below:

In this algorithm, if the user enters a variable key length of a key which is less than 64bits, then by default the program code fills in number of 0's to make it equal to 64bits. Suppose taking an example, if the user enters only "A" in place of key, the ASCII value of "A" returns 65. The value of "A" when changed into binary is (01000001). The leftover values in the key are replaced with 0's to make it equivalent to 64bits. Now as thing algorithm encrypts data N times and also requires N different keys to perform the encryption.

B.Plaintext Encryption Process

In this plaintext encryption process, the plaintext can be of variable length as stated earlier in the key generation process. In the encryption process user enters data and key of any size. And then making it equal to 64bits the encryption is being performed. Now, the key used in this plain text encryption uses a right circular process which then generates the new key [3]. The newly developed key goes again through the encryption process of the ODES algorithm and it works on till N times.

The encryption algorithm process shows how one process turns in as an input for the other process. Here, the value of N can be decided by the user and it is also sent in encrypted form so that it cannot be detected by the user.

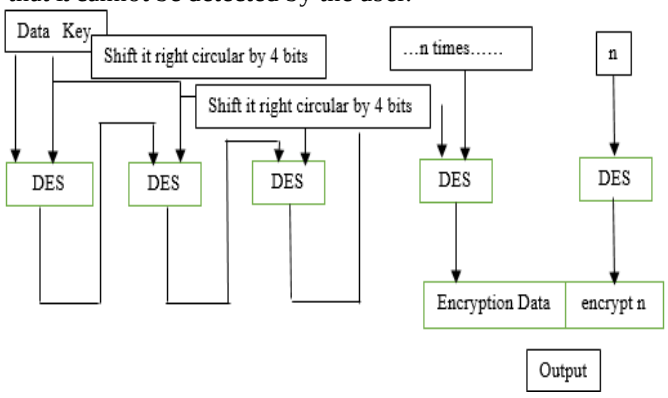

Fig. 6: Encryption Algorithm Process

C. Decryption Process

In the decryption process, the same algorithm is used in reverse order. The ODES algorithm is designed in a way so when implemented, results in decryption of the cipher text to the plain text [4]. The right circular process is being performed while encryption whereas the left circular process is performed in the decryption process. If the resultant decrypted text is less than 8bits, then (*) is appended to complete the 8bits.

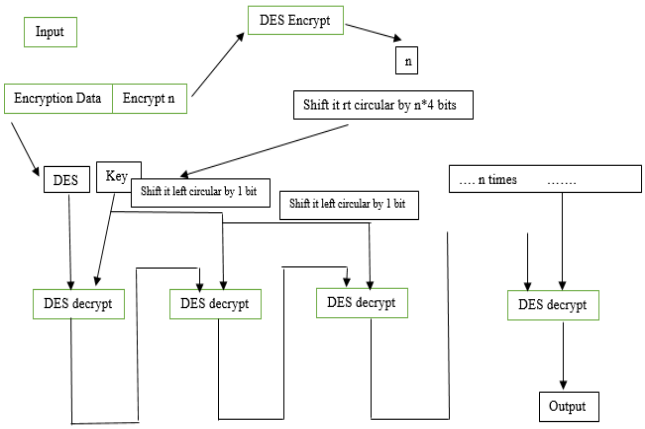

Fig. 7: Decryption Algorithm Process

VI. IMPLEMENTATION

The implementation of the newly designed ODES algorithm is done by designing a GUI interface wherein the user effort is required to perform the encryption and decryption successfully. The user needs to enter key and data of variable length. After entering the desired key and data, the "Encrypt Text" button needs to be pressed, which changes both the key and data into a specified form and performs various permutations, inverse permutations and S-Box operations [7] resulting in binary form of the cipher text. For decryption, the button "Decrypt Text" needs to be pressed which gives the output in the original form (plaintext). The operations performed on data are shown in the "Console" area. The snaps of the interface are represented below:

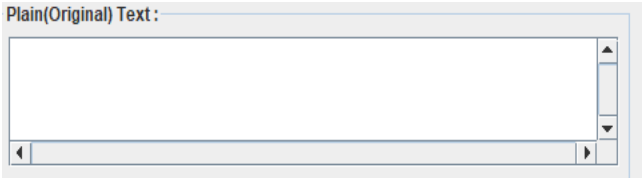

Fig. 8: Block for plaintext

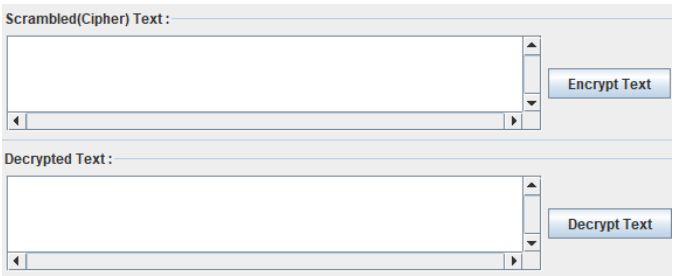

Fig. 9: Output of Cipher text and plain text

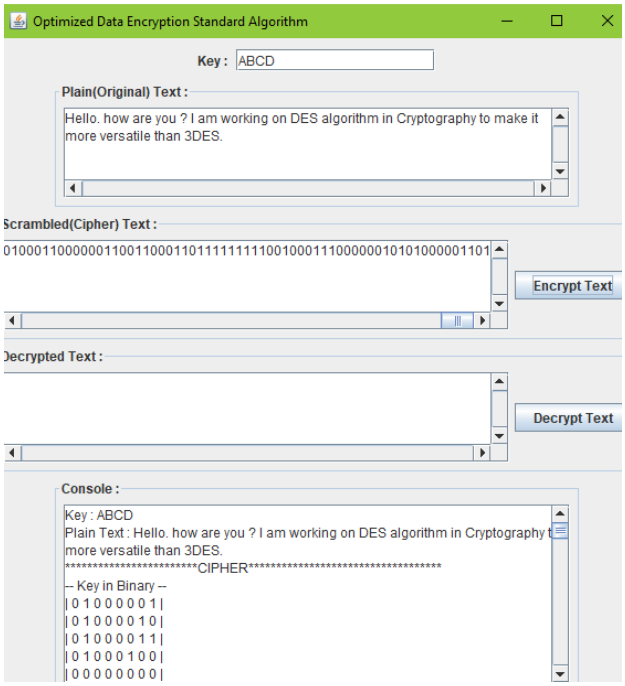

Fig. 10: ODES Interface showing Encryption

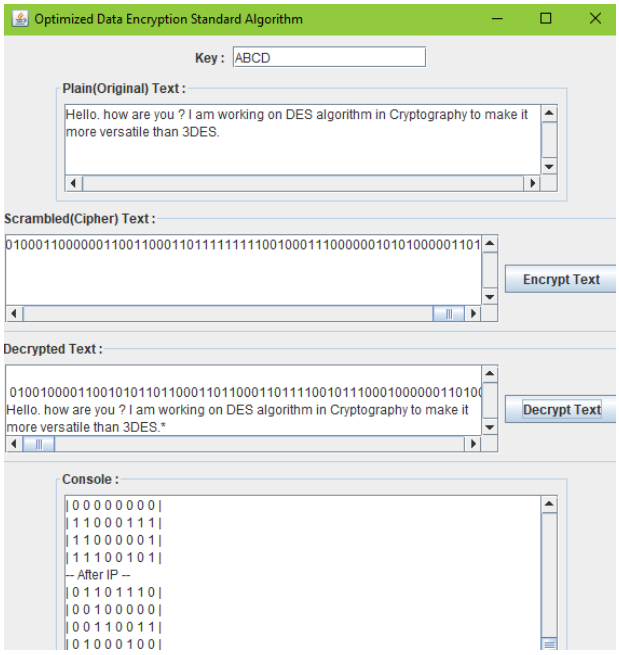

Fig. 11: ODES Interface showing Decryption

VII. COMPARISON BETWEEN DES, 3DES AND ODES ALGORITHM

There are many notable points which describe the main differences between the algorithms (DES, 3DES and ODES). The difference in between these algorithms is calculated based the key and data size used by the user as an input. The new algorithm (ODES) fills 0's in the place of the key and data left blank by the user which was not there in the DES and 3DES algorithms [6]. In addition, there is also some difference based on the decryption time in between these algorithms.

TABLE I
SHOWING COMPARISON BETWEEN DES, 3DES AND ODES

Properties	**DES**	**3-DES**	**ODES Algorithm**
Data Size	Fixed	Fixed	Variable
Key Size	Fixed	Fixed	Variable
No. of keys needed to insert	1	3	1
Decryption time	2^52	2^156	2^(N*52)
Rounds	16 rounds	48 rounds	N*16 rounds
User effort	Requires more user effort	Requires more user effort than DES	Requires less user effort than DES

VIII. CONCLUSION AND SUMMARY

This research of ODES algorithm will help in increasing the security of the data. The code applied to key and data provides more security as compared to DES and 3DES algorithm [5]. The interface so designed and used here is also very user friendly. The user need not take any pain just he needs to enter the key and data he wants to encrypt. Rest is all done by the code of the algorithm, and to get output he/she needs to press buttons and see the result in respective areas. Few of the properties of the algorithm are listed below:

- User can enter variable size data which was not possible in case of DES and 3DES algorithm.
- User can enter variable size key.
- Complexity of this algorithm increases than the previous algorithms.

IX. ACKNOWLEDGMENT

We would like to extend heartfelt gratitude to VIT University for providing us the platform to write papers and also to International Forum of Engineers and Practitioners for publishing our paper. We are also grateful to our family, friends and relatives for their blessings and support.

REFERENCES

[1] Zughoul, O., & Jani, H. M. Proposing an Encryption Algorithm based on DES.

[2] Singh, S., Maakar, S. K., & Kumar, D. S. (2013). Enhancing the security of DES algorithm using transposition cryptography techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(6), 464-471.

[3] Akhila, S. R. (2016). A Study on Most Used Cryptographic Algorithms. Suman, G., & Krishna, C. (2013). Improved Cryptosystem Using SDES Algorithm with Substitution Ciphers. *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN, 2277*.

[4] Ghnaim, W. A. E., Ghali, N. I., & Hassanien, A. E. (2010, October). Known-ciphertext cryptanalysis approach for the Data Encryption Standard technique. In *Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on* (pp. 600-603). IEEE.

[5] Sharma, A. K., & Sharma, H. (2015). NEW APPROACH TO DES WITH ENHANCED KEY MANAGEMENT AND ENCRYPTION/DECRYPTION SYSTEM (DES ULTIMATE). *International Journal of Advances in Engineering & Technology*, *8*(3), 368.

[6] Han, S. J., Oh, H. S., & Park, J. (1996, September). The improved data encryption standard (DES) algorithm. In *Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium on* (Vol. 3, pp. 1310-1314). IEEE.

[7] Rakeshkumar, S. K. Performance Analysis of Data Encryption Standard Algorithm & Proposed Data Encryption Standard Algorithm. *International Journal of Engineering Research and Development, e-ISSN*, 11-20.