TRIPLE TIMES DES

Atul Kumar

Master of Computer Science and Applications ,

Department of Computer Science and Applications,

Reva University Bangalore, India

***Abstract*— In the modern environment, almost all digital services, like internet communication, military imaging systems, medical, and multimedia systems require a high level of security and protection. We will safely and effectively share records between clients. To kept up security between clients, an verification and authorization this strategy is utilized. Clients can transfer records to the database which can be put away inside the database and after that Era of OTP are planning to be done by Triple DES. The client will download the records utilizing OTP which they gotten. After confirmation of OTP, the record be attending to be downloaded to the client. To hide the files in this system, we deployed Triple DES (Data Encryption Standard). This type of encryption technique aids in the prevention of both active and passive attacks.**

As an outcome, it's the advantage of proven reliability also as a extended key length, which eliminates many of the shortcut attacks which will be wont to reduce the quantity of some time it takes to interrupt Data Encryption Standard.

Keywords: DES, AES, Triple DES, Encryption, Decryption, OTP

I. INTRODUCTION

Since of expanding dangers to organized computer frameworks, there's awesome require for security advancements Information Encryption Standard (DES) may be a piece cipher calculation. Which is comparative to 16-hexadecimal numbers. To do the encryption, Information Encryption Standard employments "keys" where clearly Sixteen hexadecimal numbers long, or clearly 64 bits long.
However, every 8th key bit is ignored within the DES algorithm, in order that the effective key size is 56 bits. Triple-Data Encryption Standard encrypts input data three times. The three keys are mentioned as K1, K2, and K3. Thus, we use the 3 key triple-DES so it's more secure and is sometimes preferred over the normal DES. The system combines this with the OTP which can even be encrypted using triple DES.

Encryption algorithms aid the process of remodel plain text into encrypted text, then back to plain text for the aim of securing electronic data when it's transported over networks. With the help of this, the hackers or other intruders were not able to access information.

Overview of Encryption and Decryption

Encryption is a process of encrypting information such as a file or email message in ciphertext, an unreadable Form without a decryption key, to prevent anyone but the intended recipient from reading that data decryption is the reverse process of converting encrypted data to its original unencrypted plaintext form. A key in cryptography can be a long string of bits used by encryption/decryption algorithms.

II. LITERATURE SURVEY

This project, "Encryption and Decryption of Files with an OTP Using Triple DES," is being implemented to provide a safe and secure method of accessing and exchanging files, as well as multi-layer security. I even have competent research and survey papers dated up to 2020 for implementing and understanding this project.
A few of the foremost papers which are reviewed and studied are mentioned below.

The authors in these papers have explained the importance of a robust authentication system, which may provide multi-layers of security to the users of the system and safeguard them against unauthorized access

Secure Record Exchange Convention (SFTP) is an intranet-based instrument that licenses for more secure record exchanges. Encryption is performed by the computer program itself amid this case. As a result, the client plays no portion in encoding or interpreting. SFTP scrambles the record amid transmission and after that decodes the scrambled information at the conclusion client. The control to scramble keys is one among the preeminent fundamental highlights of SFTP. The record is presently scrambled and utilizing a private key amid scrambled record exchange. The Secure Record Exchange Convention creates the private key from the client's enlistment data. To translate the scrambled record, the key must be communicated by the sender to the conclusion client. As a result, the scrambled record is dispatched in conjunction with the private key. To ensure the private key, encryption is utilized. That's a inactive computer program key scrambles the

private key. As a result, with this key, the conclusion client can rapidly decode the substance. As a result, the scrambled exchange is quicker than SSH. Usually the term "Screen Share" reference to when two or more people share their screens remotely systems.

[2] Amid this paper to upgrade the Key Plan Strategy, a particular FORTIS calculation is proposed amid this inquire about in comparison to the display Triple-DES, the Verilog code was mimicked and hence the Physical plan was made utilizing Cadence Plan Suite, with the control and are having a insignificant result. The algorithm's control follows were obtained utilizing Chip whisperer R -Lite (CW1173) utilizing the CW-305 Artix-7 FPGA board since the target to work out the algorithm's control. Presenting a comparator and a flexible shifter inside the key plan calculation made it more troublesome to distinguish the operation from the control bend, diminished the PGE esteem, and made the calculation non-functional.

[3] The AES calculation, or chaotic arrangement, is utilized to scramble and unscramble pictures in this consider. The encryption and unscrambling forms are effectively executed utilizing JAVA coding. to form beyond any doubt the viability of the encryption strategy utilized, histogram investigation and adjoining pixel autocorrelation are performed on the photographs. As a result, the encryption approach can withstand a determination of assaults, counting brute constrain, cipher, and plaintext assaults.

[4] The creator of this term paper has proposed that this strategy is best when connected at the organizational level. due to the Triple-DES approach utilized, yet the information is hacked, the programmer won't be able to get to the account. As a result, this tool is that the only for security. to watch clients of Gmail, Quick Share, PayPal, eBay, and other administrations from being hacked to halt individuals from losing information on the online. the utilization of two-factor confirmation progresses security.

[5] The creators of the inquire about papers have recommend the going with information and comments illustrate that how come Triple-Des gives distant better much, better and higher and a stronger an improved a higher encryption and decoding execution prepare than DES. When we're amid a rush, this gets to be a genuine blemish. utilizing a organize to execute a few forms the minute has arrived are getting to be improved inside the longer term for the Triple-DES prepare errand would moreover incorporate a distant way better level of confirmation for all sorts of mixed media, quality and execution are basic information. The last mentioned includes scrambling information utilizing cross-platform video and sound records and different calculations.

III. METHODOLOGY

The framework requires input key (64 bits). This will be changed over to double esteem and after that 56-bit key is created bit is put at each indeed put and is set at each odd put of 56-bit piece. 1) Separate the result into two portion (28 bit each) (C0 and D0) 2) To get C1 and D1, perform cleared out move to the past comes about. 3) Discover the esteem of K1 where K1= C1 || D1. Pipe (||) shows the join. 4) Combine C1 and D1 to urge a 56-bit piece and use this can be the input for the following circular to urge C2 and D2, C3 and D3, etc. 5) In a 56-bit piece, each indeed bit is supplanted by 1 and each odd position is supplanted by bits

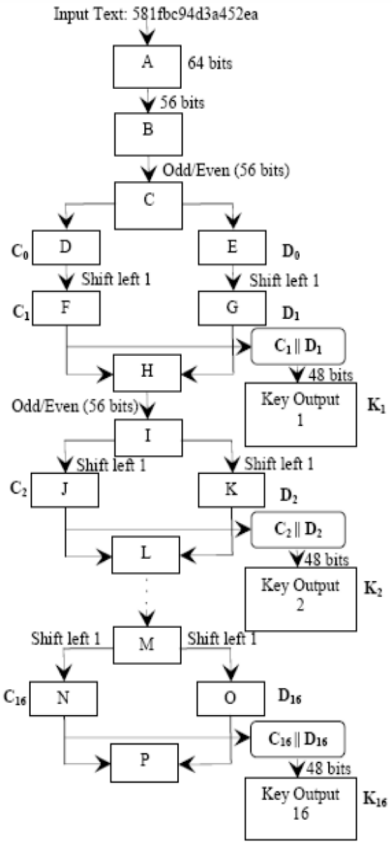
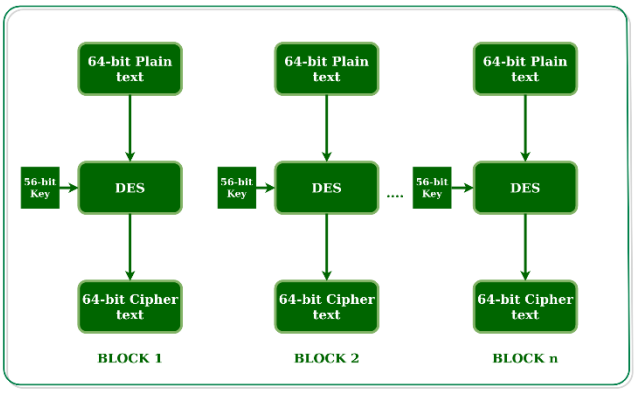


Fig 4: Key generation process

IV. DATA ENCRIPTION STANDARD ALGORITHM

DES could be a piece cipher and scrambles information in 64-bit pieces, which suggests that 64-bit of plaintext are entered as input to DES, yielding 64-bit of ciphertext. The same calculation and key are utilized for encryption and unscrambling, with slight differences. Here we utilize the length of the is 56-bit. As you'll be able see in this Fig.



We mentioned that DES uses a 56-bit key. Actually, the original key consists of 64 bits. However, before the DES process begins, every eighth bit of the key is discarded to produce a 56-bit key in this bit positions 8, 16, 24, 32, 40, 48, 56 and 64 are ignored.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

DES is based on two basic properties of cryptography:
Substitution (confusion) and displacement (Diffusion). FROM consists of 16 stages, each stage is called a round Algorithm:
1. In the first step, the initial 64-bit plain text block is back to the original Permutation (PI) function.
2. The initial permutation is performed on plain text.
3. Initial permutation produces two halves of permutation Block: Left Plain Text (LPT) and Right Plain Text (RPT).
4. Now each LPT and RPT goes through 16 rounds encryption process, each with its own key:
a. 56-bit keyword, another 48-bit subkey is generated using key conversion.
b. Using extended permutation, the RPT is changed from 32 bit to 48 bits.
c. Now 48-bit key is XORed with 48-bit RPT and the output is passed to the next step.
d. By using S box substitution, 32 bits are generated 48-bit word.
e. These 32 bits are swapped using P Box Permutation.
f. Output of P Box is XORed with LPT which is 32 bits.
g. The result of XORed (32 bit) becomes RPT and the old RPT becomes LPT. This process is called as an exchange.

3.2 Double DES

Two DES are like DES, but some processes repeat twice by two keys i.e. K1 and K2. The first is K1 key is applied on plain text and it is converted to ciphertext, then key K2 is applied to produce the result cipher text.

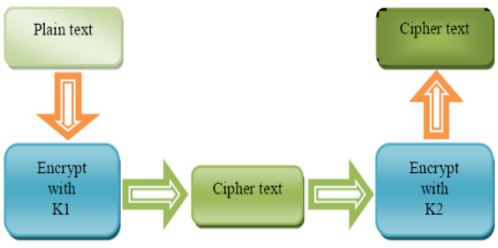


Fig 2: Encryption process using two keys K1 and K2

3.3 Triple DES

Triple DES is triple DES, in 3 DES is plain text block P is first encrypted with the key K1, then encrypted with the second key K2 and finally with the third key K3, where K1, K2 and K3 is different from each other.

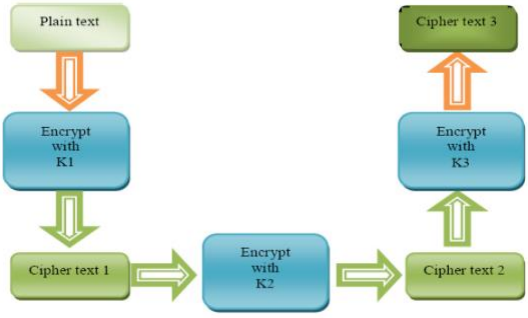


Fig 3: Encryption process in Triple DES with three keys K1 , K2 and K3.

V. CONCLUSION

In this extended abstract, we try to improve the usability of our 3DES method and I believe that Triple-DES Algorithm has proven itself to be more secure than DES Algorithm for securing our data. With its significant key size, it is very effective against brute force attacks. So, it is recommended to use Triple DES Algorithm as an encryption algorithm.

REFERENCES

1] Journal for Research| Volume 02| Issue 02 | April 2016 ISSN: 2395-7549 All rights reserved by www.journalforresearch.org 8 Securing Digital Images using Watermarking Technique and Triple DES Algorithm M.R.M Veeramanickam Varsha Khenat, Puja Dhalpe Navin Dube.

[2] International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014 Licensed Under Creative Commons Attribution CC BY Data Encryption and Decryption by Using Triple-DES and Performance Analysis of Crypto System Karthik. S, Muruganandam. A

[3] International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014 38 Image Encryption using Simplified Data Encryption Standard (S-DES) Sanjay Kumar, Sandeep Srivastava

[4] Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-5, 2017 ISSN: 2454-1362, http://www.onlinejournal.in Imperial Journal of Interdisciplinary Research (IJIR) Page 969 Image Encryption using Triple-DES Algorithm Anup R1 & Suchithra R2

[5] International Journal of Computer Applications (0975 – 8887) Volume 165 – No.8, May 2017 1 Secure Message Transfer using Triple-DES Somya Gar