|  |  |  |
| --- | --- | --- |
|  | ***INDEX*** |  |
| **Sr. No.** | **Description** | **Page No.** |
|  | **Abstract** | i |
|  | **List of Figures** | ii |
|  |  |  |
| **1** | **Chapter 1 Introduction** |  |
|  | **1.1** Introduction | 1 |
|  | **1.2 Cryptography** | 1 |
|  | ***1.3 Encryption and Decryption*** | 2 |
|  | ***1.4 Difference between encryption and decryption*** | 2 |
| **2** | **Chapter 2 Review of Literature** |  |
|  | **2.1 DES Introduction** |  |
|  | **2.2 History** |  |
|  | **2.3 Overview** |  |
|  | **2.4 ARCHITECTURE OF DES** |  |
| **3** | **Chapter 3 Comparative Analysis** |  |
|  | ***3.1 Double Data Encryption Standard*** |  |
|  | **3.2 PROPOSED METHOD** |  |
|  | ***3.3 Triple DES and improvement over original DES.*** |  |
| **4** | **Chapter 4 Design Details** |  |
|  | **4.1 Why Triple Data Encryption Standards** |  |
|  | **4.2 Triple Data Encryption Standards** |  |
|  | **4.3 ARCHITECTURE OF Triple DES** |  |
|  | **4.4 Algorithm of TDES** |  |
| **5** | **Chapter 5 Summary** |  |
|  | **5.1 Triple DES Modes of Operation** |  |
|  | **5.2 Advantages Of TDES** |  |
|  | **5.3 Disadvantages Of TDES** |  |
| **6** | **Chapter 6 References and Conclusion** |  |
|  | **6.1** Conclusion |  |
|  | **6.2** References |  |
|  | Acknowledgement |  |

***ABSTRACT***

***In today’s world all digital services like internet communication, medical and military imaging systems, the multimedia system needs a prominent level and Protected security. There is a need for a security level to safely store and send digital images holding critical information. This is because of the faster growth in multimedia technology, the internet, cell phones. Therefore, there is a need for image encryption techniques to hide images from such attacks. In this system, we use Triple DES (Data Encryption Standard) to hide images.***

***Such Encryption Tech technique helps avoid Active and Passive Attacks. The triple-DES algorithm is based on The DES algorithm itself it uses the same method as that of the DES but the difference is that it uses 3 keys rather than just one. For the encryption process, it initially encrypts the data using just one key and then decrypts the data using another different key and then finally encrypts the data again using another key. For the decryption process, it is the reverse of the encryption process it initially decrypts the cypher data using one key, then encrypts the data using another key and then finally decrypts the data back to its original form using another different key. This algorithm uniquely defines the mathematical steps needed to transform the image into a cryptographic cypher and to transform the cypher image back to its original form.***

***List of Figures***

***Fig 1.3 Encryption and Decryption Process***

***Fig. 2.3 Encryption and decryption with DES***

***Fig. 2.4 General structure of DES***

***Fig 3.1 ARCHITECTURE OF Double DES***

***Fig 4.3 Architecture OF Triple DES***

**CHAPTER 1**

**INTRODUCTION**

**1.1 Introduction to the Topic:**

In this era of universal electronic connectivity, the possibility of data damage or stolen is extremely high that is why it is needs time is to secure data from those groups. The tremendous growth in computer systems and interconnection with networks have increased depending on company or individual based on information stored and communicated using this system. There is a need to protect the data from disclosure and to protect systems from network-based attacks.

**1.2 Cryptography**

Cryptography is a technique which is intended to transform the data and can be used to supply various security related concepts such as confidentiality, data integrity, authentication, authorization, and non-repudiation. Secure the information and other services is important thing by using the security mechanism we must protected from unintended or unauthorized access, change or destruction. Cryptography is the art of secret writing to hide information secret or keeping message secure. A secure network must have integrity, so that all the information stored in always correct and protected without any redundant data. Which are used to reduce network threats.

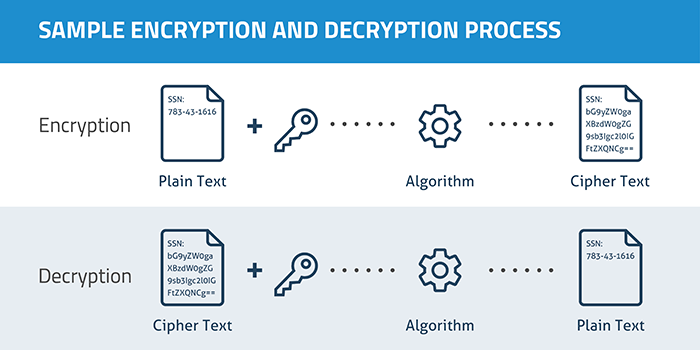
Encryption/decryption are the fundamental function of cryptography, which is used to hide the information from the unauthorized users so that chances of threats also reduced. The aim of many cryptosystems is to make their data computationally infeasible to crack by intruders. It can supply integrity as it can be used to detect any changes which may have happened to the data, and it can supply accountability as it can be used to verify the origin of the data. In encryption simple message (the plaintext) converted into unreadable form called cipher text (scrambled message after encryption). While decryption the cipher text is converted into plain text (original form) Many encryption algorithms are widely available and used in information security.

***1.3 Encryption and Decryption***

***Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That is why a hacker is not able to read the data as senders use an encryption algorithm. Encryption is usually done using key algorithms.***

***Data is encrypted to make it safe from stealing. However, many known companies also encrypt data to keep their trade secret from their competitors.***

***Decryption is a process of converting encoded/encrypted data into a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.***



***Fig 1.3 Encryption and Decryption Process***

***1.4 Difference between encryption and decryption***

|  |  |  |
| --- | --- | --- |
| ***Sr. No.*** | ***Encryption*** | ***Decryption*** |
| ***1.*** | ***Encryption is the process of converting normal message into meaningless message.*** | ***While decryption is the process of converting meaningless message into its original form.*** |
| ***2.*** | ***Encryption is the process which take place at sender’s end.*** | ***While decryption is the process which take place at receiver’s end.*** |
| ***3.*** | ***Its major task is to convert the plain text into cipher text.*** | ***While its main task is to convert the cipher text into plain text.*** |
| ***4.*** | ***Any message can be encrypted with either secret key or public key.*** | ***Whereas the encrypted message can be decrypted with either secret key or private key.*** |
| ***5.*** | ***In encryption process, sender sends the data to receiver after encrypted it.*** | ***Whereas in decryption process, receiver receives the information (Cipher text) and convert into plain text.*** |

**CHAPTER 2**

**REVIEW OF LITERATURE**

**2.1 DES Introduction**

DES (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses of DES, which made it an insecure block cypher. It has a key size of 56 bits. The problem with DES it has only 256 of combinations

Double DES which applies the algorithm twice to the plain text with a different key each time.

C=Enc (K2, Enc (K1, P))

P=Dec (K1, Dec (K2, C))

It has 2112 of combinations. Due to the MITM attack (Man in the middle) it lowers the attack complexity of finding the key easily, attacker can find out keys in less time. It has O (256).

**2.2 History**

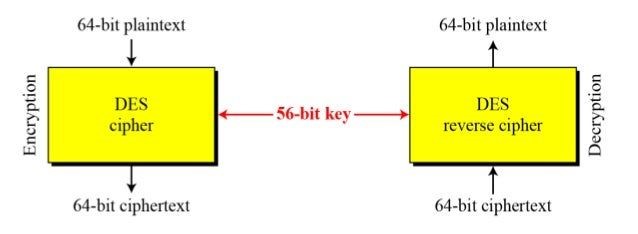
In 1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard (FIPS).

After the publication, the draft was criticized severely for two reasons. First, critics questioned the small key length (only 56 bits), which could make the cypher vulnerable to a brute-force attack. Second, critics were concerned about some hidden design behind the internal structure of DES. They were suspicious that some part of the structure (the S-boxes) may have some hidden trapdoor that would allow the National Security Agency (NSA) to decrypt the messages without the need for the key. Later IBM designers mentioned that the internal structure was designed to prevent differential cryptanalysis.

DES was finally published as FIPS 46 in the Federal Register in January 1977. NIST, however, defines DES as the standard for use in unclassified applications. DES has been the most widely used symmetric-key block cypher since its publication. NIST later issued a new standard (FIPS 46-3) that recommends the use of triple-DES (repeated DES cipher three times) for future applications. As we will see in Chapter 7, AES, the recent standard, is supposed to replace DES in the long run.

**2.3 Overview**

DES is a block cipher, as shown in Fig. 2.3.

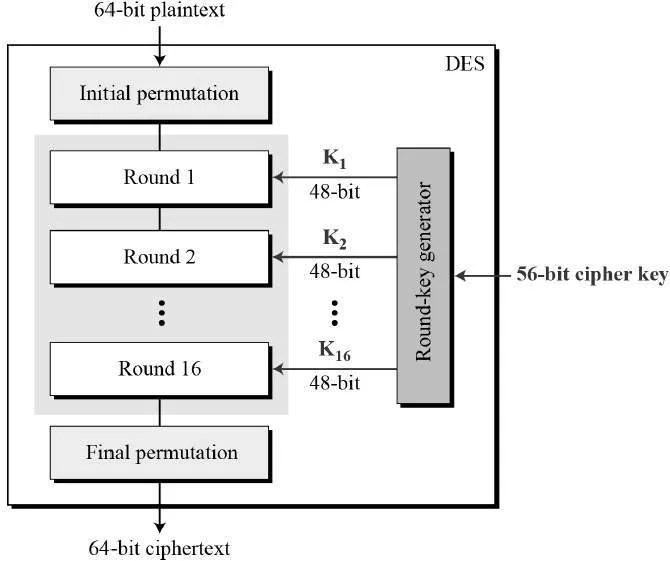


***Fig. 2.3 Encryption and decryption with DES***

At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext; at the decryption site, DES takes a 64-bit ciphertext and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption.

**2.4 ARCHITECTURE OF DES**

Let us concentrate on encryption; later we will discuss decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm described later in the chapter. Figure 2.4 shows the elements of DES cipher at the encryption site.



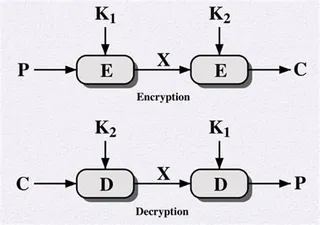
***Fig. 2.4 General structure of DES***

**CHAPTER 3**

**COMPARATIVE ANALYSIS**

***3.1 Double Data Encryption Standard***

***Double DES is an encryption technique that uses two instances of DES on the same plain text. In both instances, it uses different keys to encrypt the plain text. Both keys are needed at the time of decryption. The 64-bit plain text goes into the first DES instance which than converted into a 64-bit middle text using the first key and then it goes to the second DES instance which gives 64-bit ciphertext by using the second key.***



***Fig 3.1 ARCHITECTURE OF Double DES***

***However double DES uses 112 bits key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.***

**3.2 Proposed Method**

An enhancement of DES and Double DES, the 3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is like the one in original DES but applied 3 times to increase the encryption level. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

***3.3 Triple DES and improvement over original DES.***

***Triple DES (3DES / 3DEA) uses 3 keys of 64-bits each, with an effective key length of 56 bits (8 bits are used for parity checking). 3DES uses a block size of 64-bits.***

***There are 3 keying modes of 3DES:***

1. ***Three independent keys: Wherein none of the keys are explicitly similar: K1≠K2, K2≠K3, K3≠K1. This is also known as 3TDEA.***
2. ***Two independent keys: Wherein K1 and K2 are explicitly different but K1 and K3 are similar. K1≠K2, K2≠K3, K3=K1. This is known as 2TDEA.***
3. ***All keys are the same. K1 = K2 = K3. This key mode when used with EDE mode of 3DES is in essence – DES.***

***There are two different operating modes of 3DES:***

1. ***EDE mode: Which functions as encrypt, decrypt, encrypt with K1, K2, K3, respectively.***

***This mode can be denoted as: C = EK1(DK2(EK3(P))). This is the used mode as it supports backward compatibility with original DES standard when used with Key option 2. Using key option 3 with EDE mode is in-fact original DES standard.***

1. ***EEE mode: Wherein plaintext is encrypted 3 times using 3 keys. This is represented as: C = EK1(EK2(EK3(P)))***

***CHAPTER 4***

***DESIGN DETAILS***

**4.1 Why Triple Data Encryption Standards**

**DES is an acronym for Data Encryption Standards. It is a technique to encrypt any plain text using a 56-bit key. Advancements in technology have led to the development of new methods that can easily crack a DES-encrypted text.**

**To prevent this, another encryption technique named Triple-DES was introduced. This method is much more secure than the original DES, and it uses a 168-bit key.**

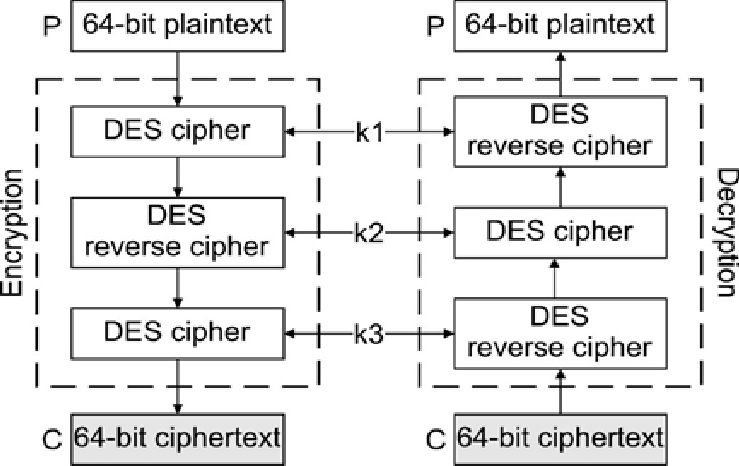
**4.2 Triple Data Encryption Standards**

**Triple-DES is a process in which we encrypt an image, text or video using 56 bit two keys or 128-bit keys. This kind of process may be secure but still has its flaws. To overcome this flaw, we encrypted out file with three 56-bit keys instead of two keys. Hence making it more secure. In the earlier referred case study, there was only two keys were used for encryption process. Triple-DES process follows EDE (Encryption, Decryption, Encryption) model. EDE model states that every file or text must be encrypted twice and decrypted once in a sequential order to perform encryption process. First it encrypts using one secret key and then decrypts using a different secret key finally encrypts using same encrypt key. So, the flaw was if the hacker got to know one secret key it is extremely easy to apply brute force attack. Hence to overcome this flaw we are using three different keys for every EDE process. EDE uses 192-bit keys out of which only 168 bits are used for encryption process.**

**Still, a strong algorithm even though we do not use the last eight bits. Which makes it more secure over a network. As the security weaknesses of DES became clearer, 3DES was proposed as a way of extending its key size without having to build an entirely new algorithm. Rather than using a single key as in DES, 3DES runs the DES algorithm three times, with three 56- bit keys:**

* + **Key one is used to encrypt the plaintext.**
  + **Key two is used to decrypt the text that had been encrypted by key one.**
  + **Key three is used to encrypt the text that was decrypted by key two.**

**4.3 ARCHITECTURE OF Triple DES**



***Fig 4.3 ARCHITECTURE OF Triple DES***

**4.4 Algorithm of TDES**

**Step1:** Choose Encryption || Decryption

**Step2: Opening file name and image**

**Step3:** Give password as Key

**Step4:**

Cipher Text = EK3(DK2(EK1(plain text)))

DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.

Plain Text = DK1(EK2(DK3(ciphertext)))

DES decrypt with K3, encrypt with K2, then decrypt with K1.

**Chapter 5**

**SUMMARY**

**5.1 Triple DES Modes of Operation**

**Experts using TDES have five different modes of operation to choose from.**

1. **Electronic Codebook (ECB). Each 64-bit block is encrypted and decrypted independently**
2. **Cipher Block Chaining (CBC). Each 64-bit block depends on the earlier one and uses an Initialization Vector (IV)**
3. **Cipher Feedback (CFB). The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit**
4. **Output Feedback (OFB). Much like CFB, except that the encryption algorithm input is the output from the preceding DES**
5. **Counter (CTR). Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each next block**

**5.2 Advantages Of TDES**

1. The image can only be viewed by the receiver as the image is encrypted using Triple DES and the key is only known to the sender and receiver.
2. Since the image is encrypted using Triple DES, it is more secure than DES.
3. Since the key is entered by the sender and receiver and is not stored in the database, it makes the encryption and decryption more secure.

**5.3 Disadvantages Of TDES**

1. The file size to be transmitted becomes large since it holds encrypted data.
2. Since the file size is huge it can be suspected to hold some critical information.

**CHAPTER 6**

**REFERENCES AND CONCLUSION**

**6.1 Conclusion**

Triple DES algorithm to encrypt and decrypt the data. This supplies a better process of secure encryption and decryption. It is more secure and faster than double DES. As it has lengthy key chances of attacking the data is less. So, it supplies security in the storage and transmission of data.

**6.2 References**

1. Aamer Nadeem, “A Performance Comparison of Data Encryption Algorithm,” IEEE 2005.
2. Abdul Kader, Diaasalama and Mohiv Hadhoud, “Studying the Effect of Most Common Encryption Algorithms,” International Arab Journal of e-technology, Vol.2. No.1.
3. Aman Kumar, Sudesh Jakhar, Sunil Makkar, “Distinction between Secret key and Public key Cryptography with existing Glitches,” Volume: 1, 2012.
4. Data Encryption Standard (DES), FIPS PUB 46-3 - 1999.
5. Feistel, Cryptography and Computer Privacy, Scientific American, Volume: 28, No.5, 1973.
6. Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003
7. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5071626&queryText=image%20thriple%20des&newsearch=true
8. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6187857&queryText=image%20thriple%20des&newsearch=true