**Diagram

Description automatically generated**

**EXPOSYS DATA LABS**

**Cybersecurity Internship Report**

Project Report on

**“Encryption of Image Using Triple DES”**

Project by:

Name: Sheefa Jalali

Email: [jalalisheefa@gmail.com](mailto:jalalisheefa@gmail.com)

Phone. No: 8951891886

**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.

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| 1. | **Introduction**   * 1. Introduction   2. Cryptography   3. Triple DES |
| 2. | **Existing Method**  2.1 DES  2.2 Double DES |
| 3. | **Architecture**  3.1 Architecture of Triple DES |
| 4. | **Proposed Method** |
| 5. | **Methodology**  5.1 Tiple DES Encryption  5.2 Triple DES Algorithm |
| 6. | **Implementation** |
| 7. | **Conclusion** |

**Chapter 1 INTRODUCION**

* 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. **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. **Triple DES:**

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.

**Chapter 2 EXISTING METHOD**

**2.1 DES Introduction**

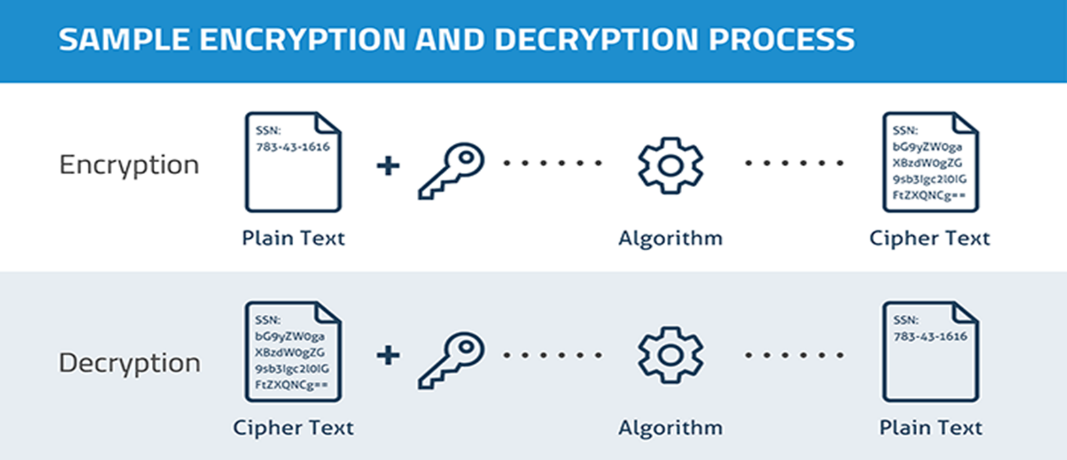
DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit the weaknesses 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).



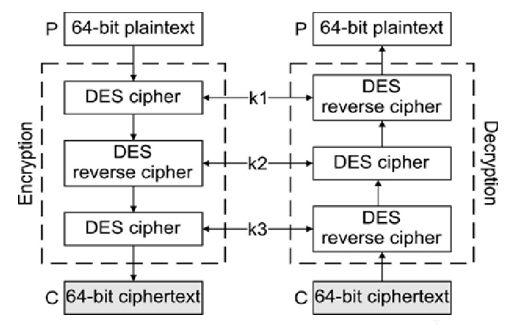
**2.2 Double Data Encryption Standard**

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. 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.

1. Has two encryption stages and two keys
2. Given a plaintext P and two encryption keys K1 and K2 and, ciphertext C is generated as C = E(K2, E(K1, P))
3. Decryption requires that the keys be applied in reverse order P = D (K1, D(K2, C))
4. This scheme apparently involves a key length of 56 \* 2 = 112 bits, resulting in a dramatic increase in cryptographic strength

**Chapter 3 ARCITECTURE**

**3.1 Architecture of Triple DES**

****

Architecture of Triple DES

It is derived from single DES, but the technique is used in triplicate and involves three sub keys and key padding when necessary, such as instances where the keys must be increased to 64 bits in length. Known for its compatibility and flexibility, software can easily be converted for Triple DES inclusion. Therefore, it may not be nearly as obsolete as deemed by NIST.  
  
Triple DES encrypts input data three times. The three keys are referred to as k1, k2 and k3. This technology is contained within the standard of ANSIX9.52. Triple DES is backward compatible with regular 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.

**Chapter 4 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. As with all block ciphers, encryption, and decryption of multiple blocks of data may be performed using a variety of modes of operation, which can generally be defined independently of the block cipher algorithm. In general, Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack, the effective security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first).

**Chapter 5 METHODOLOGY**

**5.1 Triple DES Encryption**

1. In cryptography, Triple DES, officially the Triple Data Encryption Algorithm, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.
2. Block sizes: 64 bits Key sizes: 168, 112 or 56 bits (keying option 1, 2, 3 respectively)
3. Triple DES is an encryption technique which uses three instances of DES on same plain text.
4. It uses their different types of keys choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

**5.2 Triple DES Algorithm**

TDES has a fixed data block size of 8 bytes. It consists of the cascade of 3 Single DES ciphers (EDE: Encryption - Decryption - Encryption), where each stage uses an independent DES sub-key.

The standard defines 2 Keying Options:

Option 1: all sub-keys take different values (parity bits ignored). The TDES key is therefore 24 bytes long (concatenation of K1, K2, and K3), to achieve 112 bits of effective security.

Option 2: K1 matches K3 but K2 is different (parity bits ignored). The TDES key is 16 bytes long (concatenation of K1 and K2), to achieve 90 bits of effective security. In this mode, the cipher is also termed 2TDES.

**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 6 IMPLEMENTATION**

1. Encrypt the plaintext blocks using single DES with key K1.
2. Now decrypt the output of step 1 using single DES with key K2.
3. Finally, encrypt the output of step 2 using single DES with key K3.
4. The output of step 3 is the ciphertext.
5. Decryption of a ciphertext is a reverse process.
6. First browse the file you want to encrypt using triple des.
7. Once the file is encrypted, a cipher key is generated.
8. The cipher key is copied and used in the next step.
9. Then choose the encrypted file for decryption and paste the cipher key.
10. The file is successfully decrypted, and the process is completed.

**Chapter 7 CONCLUSION**

Triple DES algorithm is used 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.