Examining THE Differences Between Symmetric Key Algorithms IN THE Context OF Encrypting AND Decrypting Images

Sudharsan G[1], V.S.Anita Sofia[2]
[1]Dept of Computer Application(MCA)
[2]Associate Professor, Dept of Computer Application(MCA)

Abstract- *To prevent unauthorised access, data is encrypted using the encryption process. Cybersecurity, which ensures the confidentiality and integrity of data transmission over the internet and provides protection against hostile assaults, is in high demand right now. In this study, the symmetric key algorithms Data Encryption Standard (DES), Triple-Data Encryption Standard (TDES), Blowfish, and Advanced Encryption Standard (AES) are compared for encryption and decryption times and throughput. The results are analysed to show that AES is a more effective algorithm for image encryption than DES, TDES, and BLOWFISH.*

Keywords- DES, TDES, BLOWFISH, AES, SYMMETRIC KEY

I. INTRODUCTION

There is a lot of information in an image. The visual processing of the information perceived occupies over a third of our cortical brain area. Images are an important source of knowledge. Photographs are used in a wide range of industries, including the storage of patient medical data, the capture of aerial photos by satellite photography, the observation of interplanetary motion by telescopes, and the preservation of an individual's identification in the form of fingerprint or iris images[1]. Medical imaging applications are one instance of how image encryption can safeguard personal information. Electronic medical records have recently been delivered through networks from laboratories to medical centres or doctors' offices to lower the cost and improve the service. Medical data, which frequently contain photos, are not permitted to be shared with unauthorized parties, per the law. Because of this, medical photos should be encrypted before being transmitted across networks. The illicit copies have cost the entertainment sector millions of dollars. Recent technological advancements make it possible to swiftly deliver multimedia to millions of homes. Satellites and the Internet will be used by the entertainment sector for multimedia delivery [2]. To overcome this type of problem encryption and decryption come into play. Encryption is the process of transforming the actual data into something meaningless(cipher) which means the actual data and transformed data have no statistical relationship between them. Decryption is a process of converting that transformed data (cipher) into actual form.

A. IMAGE ENCRYPTION:

By using a secret key, image encryption transforms a plain image into an encrypted one. By using the secret key, the decryption procedure converts the cipher image back to the original image. Decryption operations are essentially the same as encryption operations; however, they are used in reverse. The use of secret keys is essential for encryption. Figure 1.1 represents the block diagram of image encryption.

Figure 1.1 Image Encryption from the sender side

B. IMAGE DECRYPTION:

Decryption is the process of restoring encrypted data to its original state. Typically, encryption is done in reverse. It decodes the data such that only a trusted user with access to the secret key or password can decrypt the information. The receiver party uses a decryption technique and a secret key to transform the encrypted image into a plain image. Decryption is the term for this procedure. Figure 1.2 represents the block diagram of image decryption[3].

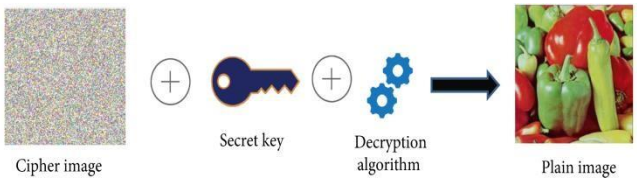

Figure 1.2 Image Decryption from the receiver side

II. METHODOLOGIES IN IMAGE ENCRYPTION

For both encryption and decryption, symmetric encryption employs the same key. In this paper, we are discussing the symmetric key algorithms used for image encryption. They are Data Encryption Standard(DES), Triple Data Encryption Standard(TDES), Blowfish and Advanced Encryption Standard.

A. DATA ENCRYPTION STANDARD (DES):

DES is a symmetric key block cipher algorithm. The Fiestel cipher is used as the DES implementation framework. There are 16 rounds of stages in the Fiestel structure. DES structures use 64 bit block sizes. Although it has a 64 bit key length, DES only uses a 56 bit key. The final 8 bits are utilized afterwards but are not utilized for encryption.

According to the approach, the encryption process uses two inputs to perform its purpose. That is an input and key in plain text. DES uses a 56 bit long key and 64 bit plain text for encryption[4].

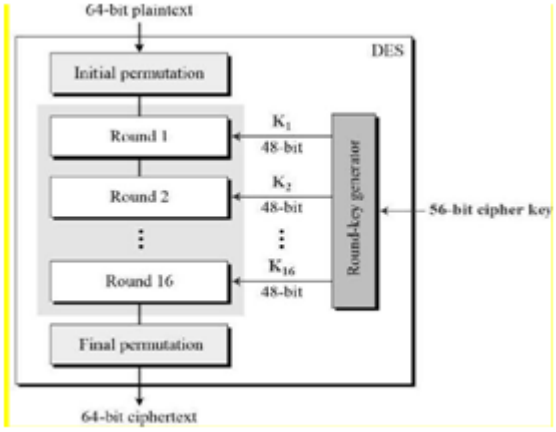

Figure 2.1 Representation of DES

All that is needed to specify DES is since it is based on the Feistel Cipher:

- Round function
- Key schedule
- Any additional processing − Initial and final permutation.

`1) DES ALGORITHM: DES is a symmetric key block cipher algorithm, as was already mentioned. The encryption and decryption steps of this technique currently use the same secret key. Plaintext 64 bit general algorithm design input. The technique converts input into a series of 64 bit encrypted text blocks. Every block of plaintext undergoes 16 rounds of encryption. The decryption process is carried out by introducing a sulky ki introduced by the main key k, where i=□ □

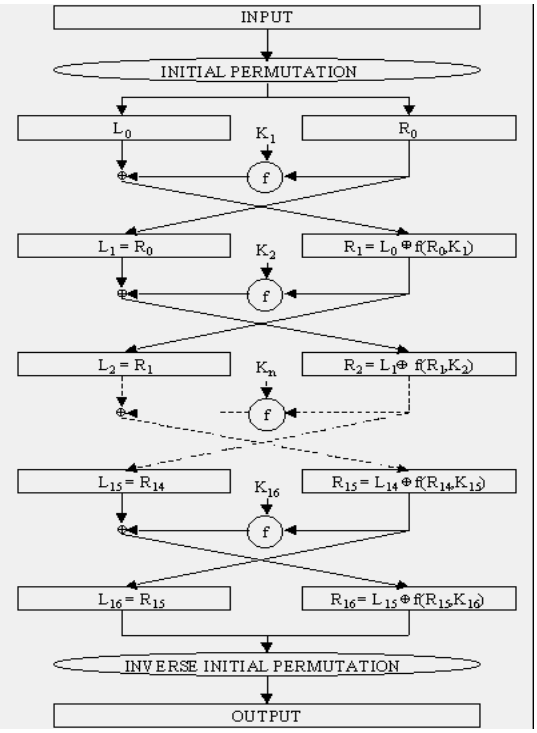

Figure 2.2 DES Algorithm Structure

Because DES uses a 56-bit key, there are 256 potential keys, making brute force unfeasible. The 8 S-boxes used in each round were kept secret, and it is also hard for anyone to learn their design, making an attack even more difficult. The algorithm's complexity rises with the number of rounds in DES. It makes the procedure slow because it needs 16 rounds for encryption and decryption. It occasionally might not be confidential because the key generation process employs random integers. As it generates 16 random keys, it uses more storage.

B. TRIPLE DATA ENCRYPTION STANDARD (TDES):

A 56-bit key is used to symmetrically encrypt data blocks using Triple DES, a more advanced version of the Data Encryption Standard (DES) algorithm. Each data block is encrypted three times using the DES cipher technique by Triple DES. UNIX passwords and ATM PINs can both be encrypted using Triple DES. Triple DES is also used by well-known programs like Mozilla Firefox and Microsoft Office[5]. Three separate instances of DES are used in the triple DES encryption method on the same plain material. It uses there different types of key 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. 8 bytes of data are encrypted using triple-DES encryption utilizing a triple-length

DATA key made up of three 8-byte DES keys: using the first key, encipher the information Use the second key to decipher the outcome. Use the third key to encipher the second outcome. To decipher data that has been triple-DES encrypted, the process is reversed: Using the third key, decipher the data. Use the second key to encrypt the final result. Use the first key to decode the second result.

1) TDES ALGORITHM: A data encryption standard known as Triple DES uses the DES cipher algorithm three times. The block size is 64 bits, and the key size is 56 bits. There are 48 DES-equivalent rounds in all. Using two keys (k1, k2) instead of one and encrypting each block twice Ek2(Ek1(plaintext)) is a naive way to boost the strength of a block encryption technique with a small key length. One would assume that this strategy would give security equal to utilizing a key that is 2n bits long if the original key length is n bits. To protect against meet-in-the-middle attacks, Triple DES employs a key bundle. It consists of three 56-bit DES keys, k1, k2, and k3.
The encryption algorithm is:

Cipher text = Ek3(Dk2(Ek1(plaintext)))

i.e., first, it will encrypt with key k1, then will decrypt with key k2, and again will encrypt with key k3.

Decryption is the reverse:

Plaintext = Dk1(Ek2(Dk3(cipher text)))

i.e., First, it will decrypt with key k3, then will encrypt with key k2, and again will decrypt with key k1[6].

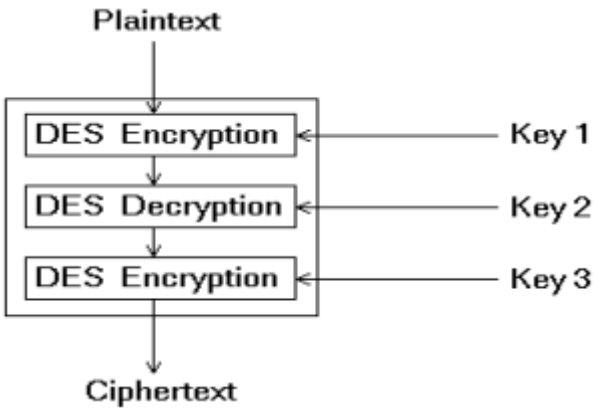

Figure 2.3 Working of Triple DES

Since the image is encrypted using Triple DES and the key is only known to the sender and receiver, only the recipient can view it. The image is more secure than DES because it is encrypted with Triple DES. Encryption and decryption are more secure because the key is entered by the sender and receiver and is not stored in the database. The file size to be transmitted becomes large since it contains encrypted data. Since the file size is huge it can be suspected to contain some critical information [7].

C. BLOWFISH:

One of the symmetric encryption techniques most frequently and successfully employed for data security is this one. Because it is not patented and requires no permission, it is accessible to all users. One of the most important and effective cryptography algorithms, with key lengths ranging from 32 bits to 448 bits. As a free, quicker alternative to established encryption methods like DES, 3DES, AES, etc., 1933 Bruce Schneider created the Blowfish algorithm. The same secret key is used for both encryption and decryption, and plaintext is partitioned into fixed-length blocks during these operations. Figured out that the blowfish algorithm is split into two parts: key expansion and data encryption. Information is encrypted. Feistel Network, which only executes the encryption algorithm in the predetermined number of iterative rounds while splitting the key expansion portion's maximum 448-bit key length into sub-keys totaling 4168-bits. Multiples of eight bytes in size make up the 64-bit block length.

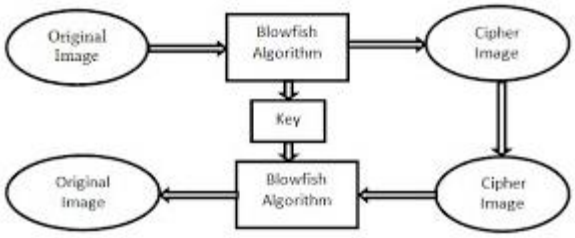

Figure 2.4 Working of blowfish algorithm

Blowfish maintains two sub-key arrays: four (4) S-boxes and eighteen (18) P-array (32-bits each) boxes (32-bits each, resulting to 256 entries). The first 32 bits of the key are exclusively XORed with the first 32 bits of the P-array after string initialization (P1). This process continues until the algorithm completes the set number of round iterations. The left (L) and right (R) are switched after the final round of iteration, and then left (L) and right (R) are XORed as the 17th and 18th indexes of the P-box, respectively. The encryption data is created from this new 64-bit output. Simply doing the encryption procedure in reverse order is what the decryption process does.

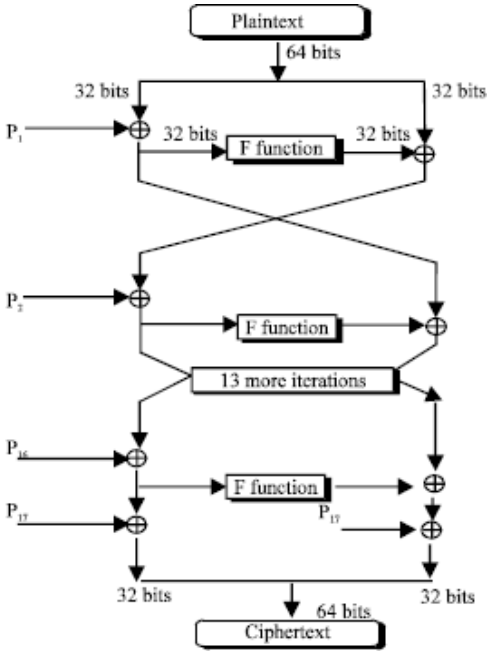

Figure 2.5 Blowfish Algorithm Structure

1)BLOWFISH ALGORITHM: The basic algorithm for Blowfish is illustrated as follows:

Divide X into two 32-bit halves XL and XR For i=1 to 16:
XL = XL Pi
XR = F (XL) XR
Swap XL and XR End for
Swap XL and XR XR = XR P17 XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)

Except when changing keys, blowfish is one of the swiftest block ciphers currently in use. When compared to other block ciphers, each new key requires pre-processing that would take around 4 kilobytes of text to encrypt. This makes it impossible to utilize in some programs, but not in others, like SplashID. It actually works to an application's advantage, especially because the OpenBSD password-hashing technique utilizes a Blowfish-derived algorithm that takes advantage of the sluggish key schedule. Since Blowfish is not covered by any patents, anyone can use it without paying anything. This has boosted its acceptance in cryptographic software.

One of Blowfish's drawbacks is that the key must be delivered to the user outside of the band, specifically over an unsafe communication channel. As more users are added, key management gets more difficult because each pair of users need a unique key. For instance, N(N-1)/2 keys are needed. Since two persons are using the same key, Blowfish cannot offer authentication and non-repudiation. Additionally, it is less efficient than other algorithms in terms of throughput and time consumption during the decryption process.

D. ADVANCED ENCRYPTION STANDARD (AES)

A symmetric block cipher algorithm with a block/chunk size of 128 bits is the AES Encryption algorithm, also referred to as the Rijndael algorithm. These distinct blocks are converted using keys that are 128, 192, and 256 bits long. It then joins these blocks to create the cipher text after encrypting each one separately. It is actually based on an SP network, also referred to as a substitution-permutation network. It consists of a number of interconnected operations, some of which involve bit shuffles and others involve substituting inputs with particular outputs (substitutions) (permutations)[8].

There are three block ciphers in AES:

A block of messages can be encrypted and decrypted using AES-128 using a 128-bit key length.
A block of messages can be encrypted and decrypted using AES-192 using 192-bit keys.
A block of messages can be encrypted and decrypted using AES-256 using a 256-bit key length.
Each cipher uses cryptographic keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits. Secret key ciphers, also referred to as symmetric ciphers, employ the same key for both encryption and decryption. The secret key must be known by both the sender and the recipient. Information is divided into three categories by the government: confidential, secret, and top secret. The Confidential and Secret levels can be secured using any key length. To safeguard the Confidential and Secret levels, any key length can be utilized. Either 192 or 256-bit key lengths are required for Top Secret information.
128-bit keys go through 10 rounds, 192-bit keys go through 12, and 256-bit keys go through 14 rounds. The input plaintext is processed through a number of phases in a round, including substitution, transposition, and mixing, to produce the final output of cipher text[9].

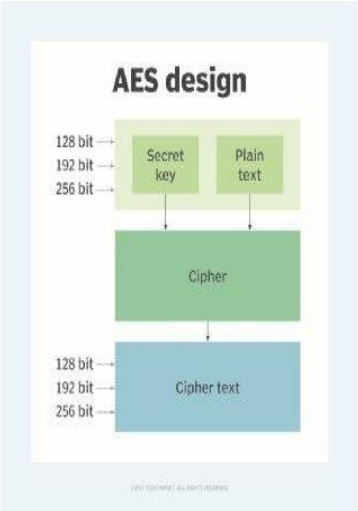

Figure 2.6 Working of AES Algorithm

1)AES ALGORITHM: The advanced encryption standard AES was first introduced by NIST in 2000. AES uses data that is 128 bits, or 16 bytes, long. The key, however, can expand to different lengths (for example, 128, 192, and 256 bits). For 128-bit, 192-bit, and 256-bit keys, respectively, AES has 10, 12, and 14 rounds.

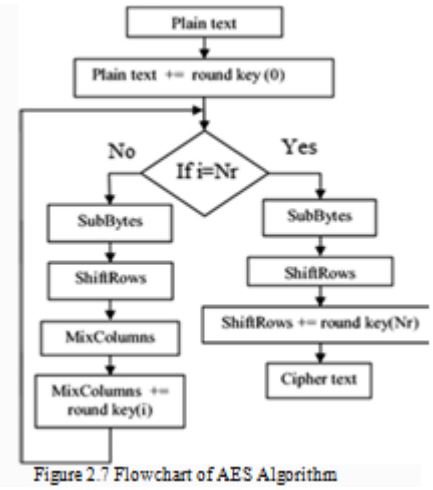

Figure 2.7 Flowchart of AES Algorithm

AES has four major operational blocks: 1. Substitute byte transformation: Each data block's byte is replaced with a different block using an S-box. 2. Row shift transformation: Depending on where it is located within the state matrix, each row is given a cyclic shift to the right side. 3. Mix Transformation of Columns: This involves multiplying each column of the state matrix by that of the fixed matrix, which is a matrix multiplication operation. 4. Add Round Key Transformation: An XOR operation is carried out between the new state matrix and the round key matrix. For encryption, it utilizes longer key sizes, including 128, 192, and 256 bits. As a result, the AES algorithm is more secure against hacking. For a wide range of applications, including wireless communication, financial transactions, e-commerce, encrypted data storage, etc., it is the most popular security protocol. One of the most widely used commercial and open source solutions worldwide. Your personal information is completely secure. Around 2128 attempts are required to break a 128-bit encryption. This makes it extremely challenging to hack, making it a very safe protocol. It uses an algebraic structure that is way simple. The encryption method is the same for every block. With software, difficult to implement. Considering both performance and security, it is difficult to implement AES in a counter mode in the software.

III. COMPARATIVE ANALYSIS

As we discussed in earlier sections about the symmetric algorithms keeping that in mind we are comparing the methods on the basis of speed, security, key size, block size, and structure.

FACTOR	DES	3DES	BLOWFISH	AES
Encryption	Slow	Slow	Fast	Fast
Decryption	Slow	Slow	Fast	Fast
Key Size	It has key size of 56 bits	It has key size of 112 or 168 bits	It has key size of448 bits	It has key size of 128,192 or 256 bits
Block Size	It has block size of 64 bits	It has block size of 64 bits	It has block size of 64 bits	It has block size of 128 bits
Developed in	1975	1978	1993	2000
Speed depends on key	Yes	Yes	No	Yes
Security	It is not secure enough	It is not secure enough	It is secure enough	It is excellent in security
Structure	It uses Feistel network as a structure	It uses Feistel network as a structure	It uses Feistel network as a structure	It uses Substitution Permutation network
Hardware and Software Implementation	Designed for efficient hardware but quite slow in software	Designed for efficient hardware and quite slow in software	Efficient in software	Efficient in both hardware and software

As the table above illustrates, DES is not sufficiently secure. It is simple to crack due to its small key length and brute force attacks. Consequently, even if 3DES is a different option, it is also insufficiently secure: Blowfish is a good option, however, its block size is insufficient compared to AES. As a symmetric key encryption method for enterprises, we see AES as DES's replacement. It will accept keys with a size of 128, 192, or 256 bits. Both the software and the hardware are effective.

IV. CONCLUSION

Every symmetric key algorithm has both strong and weak areas. We choose the encryption algorithm depending on

the requirements of the intended application. The blowfish algorithm, which records the shortest time among all algorithms, is the best option in terms of time and memory according to the criteria of guessing attacks and the required features, according to the experimental findings and comparison. Additionally, it uses the least amount of RAM. AES algorithm can be chosen if secrecy and integrity are important considerations. The optimum choice is DES if network bandwidth is required by the application. The blowfish and AES algorithms can be used on top of all IPv4 and IPv6-based internet protocols to protect applications from guessing attacks, and tests conducted for this paper show that all of the classes and algorithms functioned properly despite having varying execution times and memory requirements.

REFERENCES

[1] Chiranji Lal Chowdhary-"Analytical Study of Hybrid Techniques for Image Encryption and Decryption"-2020
[2] Ashish S. Dongare-"An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application"-2017
[3] Mandeep Kaur-"Computational Image Encryption Techniques: A Comprehensive Review"-2021
[4] Manjula K G-"Color Image Encryption and Decryption Using DES Algorithm"-2016
[5] URL-https://www.getapp.com/resources/common-encryption-methods/
[6] Mr. Jawwad A R. Kazi-"REVIEW PAPER ON IMPLEMENTATION OF TRIPLE DES USING OTP"-2019
[7] URL-https://nevonprojects.com/image-encryption-using-triple-des/
[8] URL-https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption
[9] URL;https://www.techtarget.com/searchsecurity/definition/ Advanced-Encryption-Standard