Exploring the Cryptographic Algorithms: A Comparative Study of DES, 3DES and AES with Various Modes of Operations

Prathima Gamini[1], A.Manikanta[2], D.B.Rohith Varma[3], G.Sandilya[4], D.Yeshwanth[5]
[*1]Assistant Professor, [*2,3,4,5]Students,
Electronics and Communication Engineering,
SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE, Chinna Amiram, Bhimavaram, Andhra Pradesh, India.

Abstract-In today's world, data security has become a major issue to the people who are using smart devices. Over the last few years some of the major technological companies were caught red-handed doing a data breach with their user's passwords. It was not just a few passwords either; that many company employees had uncontrolled access to user's data and some took advantage of it for their personal interest. In this paper, in-order to secure the data during communication, data storage, transmission encryption and decryption methods such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) algorithms were discussed.

KEYWORD- DES,3-DES, AES, Modes of operations.

I.INTRODUCTION

Professionals make a distinction between ciphers and codes. A Cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Cryptography techniques are being used by the military, the diplomatic corps, diarists etc.

The art of protecting information by transforming it into an unreadable format or method of protecting information and communication with codes, so that only the intended users can read and process it. More generally cryptography is about constructing and analyzing protocols that prevent third parties or the public reading private messages, thereby enhancing confidentiality.

TYPES OF CRYPTOGRAPHY

1.**Symmetric cryptography:**

It is the symmetric kind of encryption technique that involves only one key to encrypt and decrypt(or cipher and decipher) information. It is also called secret key cryptography or private key cryptography. The most popular symmetric key cryptography system is DES(Data Encryption Standard).

2.Asymmetric key cryptography:

It is also called public key cryptography. It uses two keys i.e a pair of key for encryption and decryption. Public key is known to every one and private key is known only to the intended user.A message that is encrypted by using a public key can only be decrypted using a private key whereas, a message encrypted by using a private key can be decrypted by a using public key.

3.Hash Functions:

There is no usage of key in this concept . It takes input message in variable length and gives fixed length output. Hash code makes it impossible for the contents of plain text to be recovered.Many Operating Systems use hash functions to encrypt passwords.

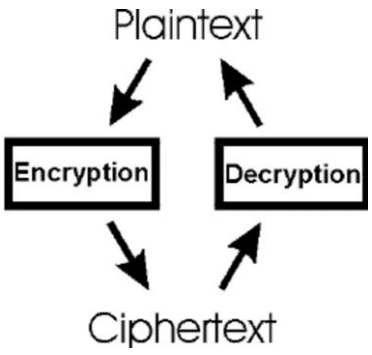

Fig.1.1.Encryption and Decryption Process

II.METHODOLOGY

The Data Encryption Standard (DES) was found vulnerable to very powerful attacks and thus, DES's popularity was fallen down. In DES, block figure the message will be encrypted into blocks of 64-bit size each, which means 64 bits of plain text is entered into DES, producing 64 bits of encrypted text. In this algorithm, same keys are used for encryption and decryption with minor differences. The key is 56 bit long. The basic idea is presented in the figure:

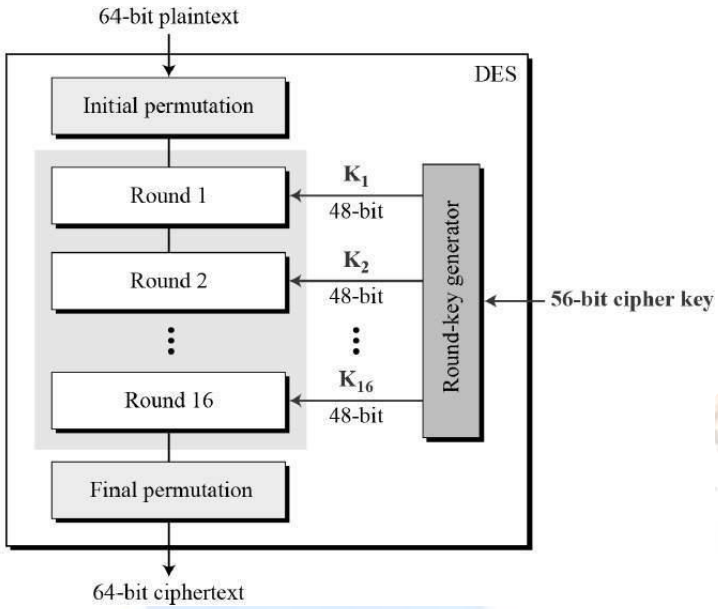

Fig.2.1.1.DES Process

In fact, the initial key is 64-bit. However, before the DES process begins, bits which were placed in multiples of 8-bit positions in this 64-bit key will be discarded resulting in a 56-bit key. That is, it rejects the 8, 16, 24, 32,40-, 48-, 56- and 64-bit positions. Thus, rejecting each 8th bit, generates a 56-bit key of the original 64-bit key.

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

Fig.2.1.2. Discording of every 8th bit of original key

DES is based on the two basic attributes of encryption: substituting (also called confusion) and transposing (also called diffusion). DES /comprises 16 stages, each of which is called a round. Each round executes the substitution and transpose steps. Now let's review the general steps of the DES.

- Initially, the 64-bit plain text block is passed to an Initial Permutation (IP) function. The initial permutation is performed on plain text.
- Then the Initial Swapping (IP) produces two halves of the swapped block: Left Plain Text (LPT) and Right Plain Text (RPT).
- At the moment, each LPT and RPT goes through 16 encryption cycles.
- Finally, LPT and RPT are reunited and the combined block is subjected to a Final Permutation (FP).
- This process generates 64-bit ciphertext as a result.

Initial Permutation (IP):

- As previously mentioned, the initial permutation (IP), which occurs prior to the first round, only occurs once. The figure illustrates how it suggests the transposition in IP should go. As an illustration, it states that the IP swaps out the first bit of the original plain text block for the 58th bit, the second bit for the 50th bit, and so on.
- All that is being done here is placing the bit positions of the original plain text block as depicted in the figure

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

Fig.2.1.3. Initial permutation table

After IP, the resulting 64-bit permuted text block is split into two half blocks, as mentioned earlier. Each of the 16 rounds is made up of the broad-level steps as shown in the figure and each half-block is made up of 32 bits.

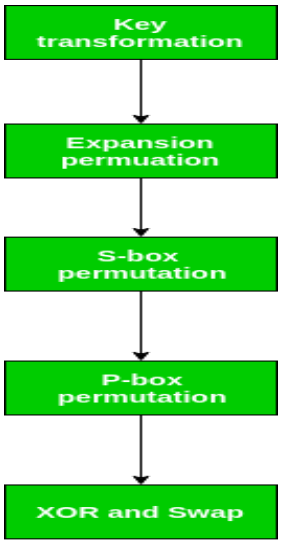

Fig.2.1.4. Broad-level steps

As mentioned, the initial 64-bit key is reduced to 56 bits by throwing away every eighth bit. Consequently, a 56-bit key is accessible for each. A procedure known as key transformation is used to create a unique 48-bit Sub Key from this 56-bit key during each round. The 56-bit key is split into two parts, each of 28 bits, for this purpose. Depending on the round, these halves have a circular left shift of one- or two-bit positions of 56 bits are chosen after the proper shift. The table is depicted in the figure below for choosing these 48 bits. For instance, bit number 14 moves to the first position after the shift, followed by bit number 17, and so on. One can observe that the table only has 48-bit positions. To reduce a 56-bit key to a 48-bit key, bit number 18 is discarded along with 7 other bits (bit number 18 will not appear in the table). Compression Permutation is the name given to the key transformation procedure because it chooses a 48-bit subset of the original 56-bit key and involves permutation.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Fig.2.1.5. Compression permutation

A different subset of key bits is utilized in each round as a result of this compression permutation technique. Due to this, DES is difficult to crack.

3DES ALGORITHM:

Block Cipher algorithms are applied three times to each data block in 3DES encryption, also referred to as Triple Data Encryption Standard (3DES). In Triple-DES, the key size is increased to provide more security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. In data encryption standards, there are three keying options.

1. All keys being independent.
2. Key 1 and Key 2 are independent keys.
3. All three keys are identical.

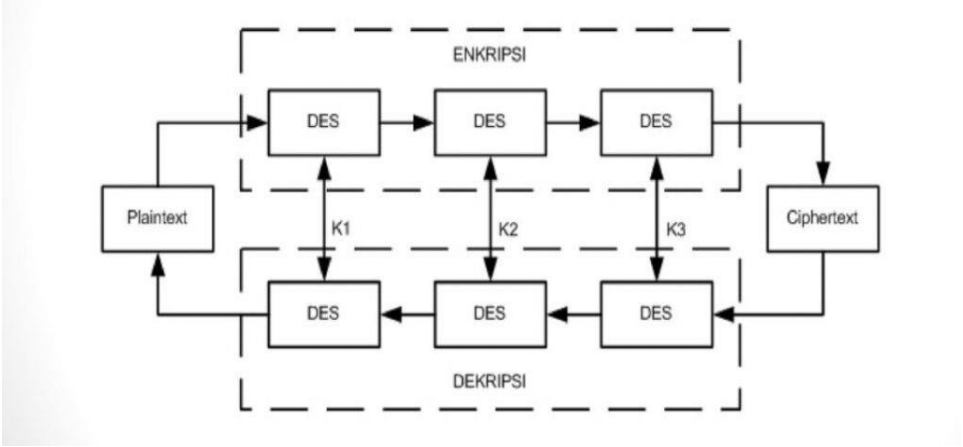

Fig.2.2.3DES Encryption

Key option #3 is known as triple-DES. Triple-DES keys have a length of 168 bits, but their security is only 112 bits. Data input is encrypted three times using triple DES. K1, K2, and K3 are the names given to the three keys. This technology is covered by the ANSIX9.52 standard. Regular DES and triple DES are backward compatible. Triple DES has a long key length, which is longer than the majority of key lengths associated with other encryption modes, making it useful. However, the National Institute of Standards and Technology (NIST) recently replaced the DES algorithm with the Advanced Encryption Standard (AES).

AES ALGORITHM:

The United States National Institute of Standards and Technology (NIST) created the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data in 2001. Despite being more difficult to implement, AES is still widely used because it is much stronger than DES and triple DES.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

Working of the cipher: Instead of operating on bits of data, AES operates on data in bytes. The cipher processes 128 bits (or 16 bytes) of the input data at a time because each block is 128 bits in size.

The number of rounds depends on the key length as follows:

- 128bit key – 10 rounds
- 192bit key – 12 rounds
- 256bit key – 14 rounds

All the round keys from the key are calculated using a Key Schedule algorithm. Therefore, many different round keys which will be used in the corresponding rounds of encryption will be created using the initial key.

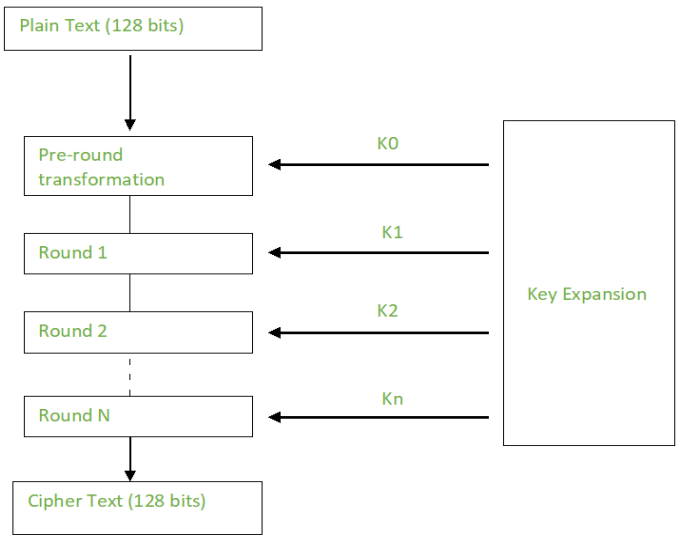

Fig.2.3.1. AES Encryption

Each round comprises of 4 steps:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The Mix Columns round is absent from the final round. In this algorithm, Sub Bytes handle substitution, while Shift Rows and Mix Columns handle permutation.

SubBytes: This action carries out the substitution. Each byte is replaced with another byte in this step. A byte is never replaced by itself or by a byte that is complement of the current byte because of the way this substitution is carried out. This process yields the same 16-byte (4 x 4) matrix as before. The permutation is applied in the following two steps.

Shift Rows: This action is straight forward. The number of shifts for each row varies. There is no shift in the first row. The third row is moved twice to the left, and the second row is moved once to the left. There is a triple shift to the left of the fourth row.

Mix Columns: This process essentially involves multiplying matrices. Each column is multiplied by a particular matrix, which changes the order of each byte in the column. The previous round omits this step.

Add Round Keys: The output of the previous stage is now XORed with the corresponding round key to produce the result. In this context, the 16 bytes are simply regarded as 128 bits of data rather than a grid.

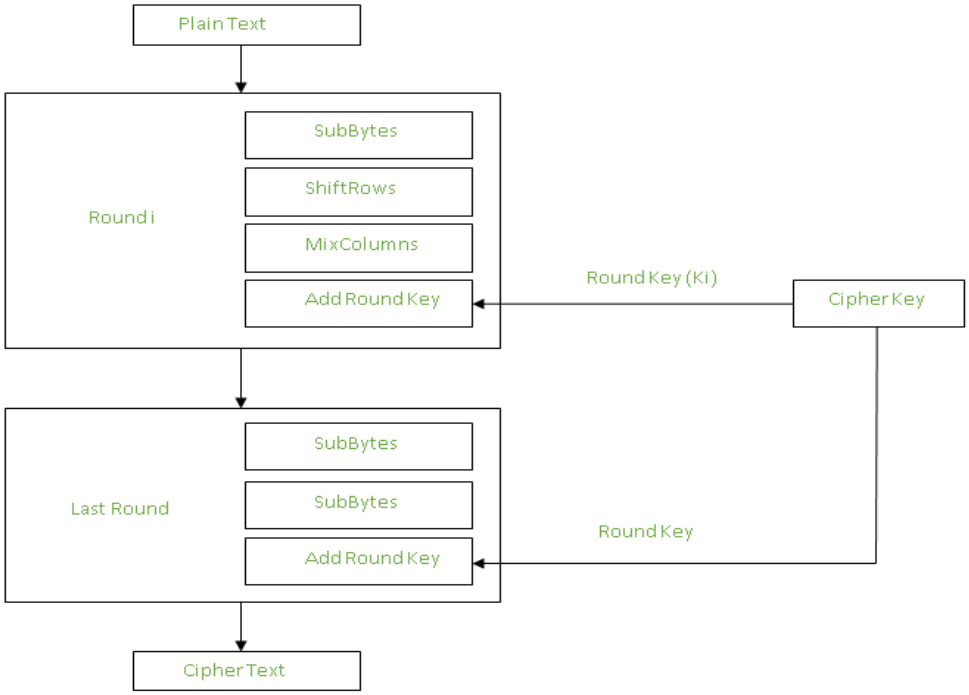

Fig.2.3.2. overview of AES Algorithm

128 bits of encrypted data are returned as output after each round. This procedure is repeated until every bit of the data that needs to be encrypted has gone through it.

Decryption:

The stages in the rounds are simple to reverse because they each have an opposite that, when used, undoes the modifications. Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.
The stages of each round in decryption are as follows:

- Add round key
- Inverse Mix Columns
- Shift Rows
- Inverse Sub Byte

The encryption process is reversed during the decryption process, so it’s outline with significant variations is discussed as below.

Inverse Mix Columns: This step is comparable to the encryption's Mix Columns step, but it differs in the matrix that is used to perform the operation.

Inverse Sub Bytes: During decryption, bytes are substituted using the Inverse S-box as a lookup table.

III.MODES OF OPERATION:

1.Electronic Code Book (ECB): The simplest way to operate a block cipher is with an electronic code book. It is simpler because each block of input plaintext is directly encrypted, and the output takes the form of blocks of encrypted ciphertext. A message can be usually divided into several blocks and the process is repeated if it is bigger than bits.

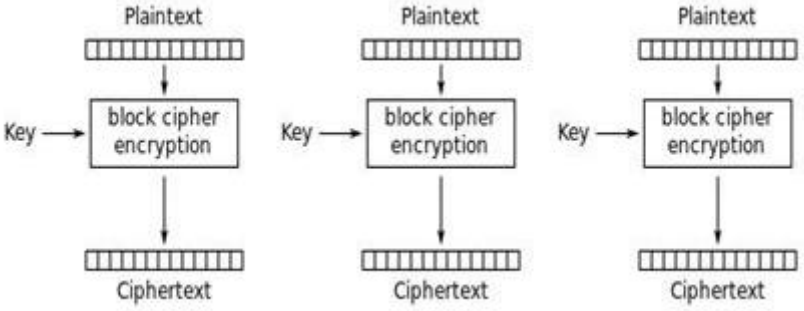

Fig.3.1. Electronic codebook (ECB) Mode Encryption

Advantages of using ECB

- Parallel encryption of blocks of bits is possible, thus it is a faster way of encryption.
- Simple way of the block cipher.

Disadvantages of using ECB

- Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

2.Cipher Block Chaining (CBC)

Cipher Block Chaining, also known as CBC, is an improvement over ECB because ECB compromises some security requirements. The previous cipher block is passed as input to the subsequent encryption algorithm in CBC after the initial plaintext block was XORed. Here, a cipher block is created in essence by encrypting an XOR output of the previous cipher block and present plaintext block.

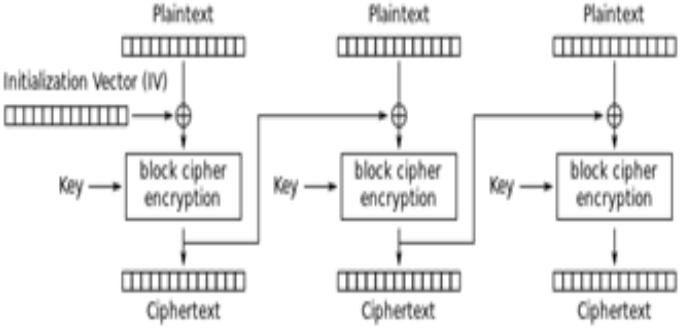

Fig.3.2. Cipher Block Chaining (CBC) mode encryption

Advantages of CBC

- CBC works well when the input consists of greater lengths.
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

Disadvantages of CBC

- Parallel encryption is not possible since every encryption requires a previous cipher.

Cipher Feedback Mode (CFB)

In this mode, the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of s and b-s bits. The plaintext bits and left-side s bits are chosen, and then an XOR operation is performed on them. The result is given as input to a shift register having b-s bits to LHS. s bits to RHS and the process continues. The following process for encrypting and decrypting the same data uses encryption algorithms.

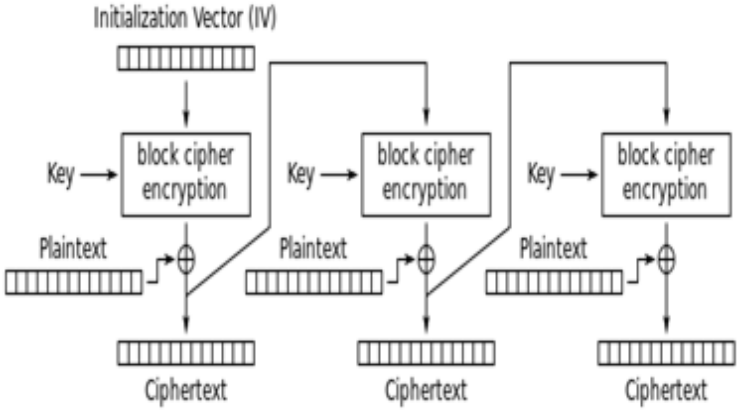

Fig.3.3. Cipher Feedback (CFB) mode encryption

Advantages of CFB –

• Applying cryptanalysis is challenging because shift register use results in some data loss.

Disadvantages of using ECB –

• The disadvantages of CFB and CBC mode are identical. The losses or multiple blocks being encrypted simultaneously. But decryption is loss encryption does not support block -tolerant and parallelizable.

IV.Conclusion:

In cryptography, operations performed for encryption and decryption process play a major role in measuring the performance such as efficiency and speed. However, based on the "mode of operation" of algorithm, it's performance itself changes and immunity of the cipher towards crypto-attack changes. DES, 3DES and AES have most of the modes of operations in common. In this paper, the operations of DES, 3DES and AES are analyzed, and modes of operation are discussed. It can be concluded that for data of one block size, one can use EBC mode. CBC and CFB are similar. However, CFB is best because one can need only encryption and not decryption, which can save code space.

V.References:

[1] 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018).

[2] DES encryption and decryption algorithm implementation based on FPGA Subhi R. M. Zeebaree Duhok Polytechnic University, Technical College of Informatics, Information Technology Department, Iraq.

[3] 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-7281-7741-0/20/$31.00 ©2021 IEEE.

[4] 2014 International Conference on Parallel, Distributed and Grid Computing, performance evaluation of various symmetric encryption algorithm.

[5] 2019 International Conference on Information and Communications Technology (ICOIACT) Effectiveness comparison of the AES and 3DES cryptography methods on email text messages.

[6] Performance Evaluation for DES and AES Algorithms- An Comprehensive Overview by S.Srilaya, S. Velampalli - 2018 3rd IEEE International 2018 - ieeexplore.ieee.org

[7] A. Nadeem and M. Y. Javed, "A encryption algorithms," in Info technologies, 2005. ICICT 2005.

[8] F2005, pp. 84-89. S. William and W. Stallings, Crypto g-Pearson Education India, 2006.

[9] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[10] Buchmann, Johannes. Introduction to cryptography. Springer Science & Business Media, 2013.

[11] Performance evolution of Various Symmetric Encryption Algorithms by Shaify Kansal, Meenakshi Mittal.

[12] Jain, R. Jejurkar, R. Chopade, S. Vaidya & Sanap, M. (2014). AES Algorithm Using 512 it Key Implementation for Secure Communication. International journal of innovative Research in Computer and Communication Engineering, 2(3).