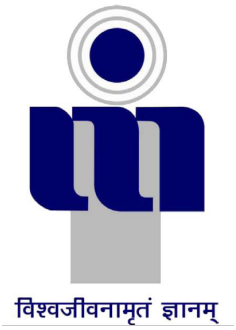
# BLOCK CIPHERS (DES, 3DES & AES)

*A case study report,*
*submitted to* **Dr. Debanjan Sadhya**
*in the subject of Information Security Systems (ISS)*

*by*

**Amal Shaji (2017BCS-010)**
**Sandarbh Yadav (2017BCS-027)**
**Vaibhav Garg (2017BCS-038)**
**Vikram Choudhary (2017BCS-039)**




**ABV INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT**
**GWALIOR-474 015**

**2019**

# TABLE OF CONTENTS

# CHAPTER 1

# Introduction

Cryptography is the branch of computer science which deals with encryption of messages. Cryptanalysis is the opposite of cryptography and deals with decryption of the encrypted messages. Both branches are a part of more general branch termed cryptology. Cryptology is the science of encryption and decryption. Figure 1.1 illustrates the classification.

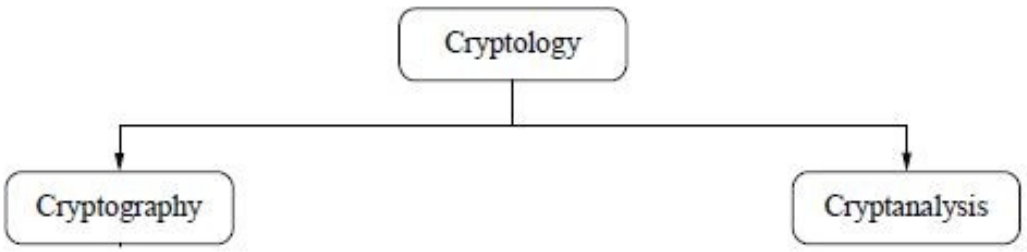



Figure 1.1: Classification of Cryptology

Cryptography is further divided into 3 branches: symmetric ciphers, asymmetric ciphers and cryptographic protocols. In symmetric ciphers, same key is used for encryption and decryption. Symmetric encryption is also known as single key encryption or **private key encryption**. In asymmetric ciphers, sender and receiver use different key system. Asymmetric encryption is also known as two key encryption or **public key encryption**. RSA, Elliptic Curve Cryptography (ECC) and Diffie Hellman Key Exchange (DHKE) use asymmetric encryption techniques. Cryptographic protocols refer to the cryptographic algorithms which ensure information security. Examples include hash functions, digital signatures, SHA-1 etc.

Symmetric ciphers can be further classified into stream ciphers and block ciphers. In stream ciphers, bits are encrypted individually by performing bitwise XOR operation of plain text bits with pseudo-random key stream. On the other hand, block ciphers en-

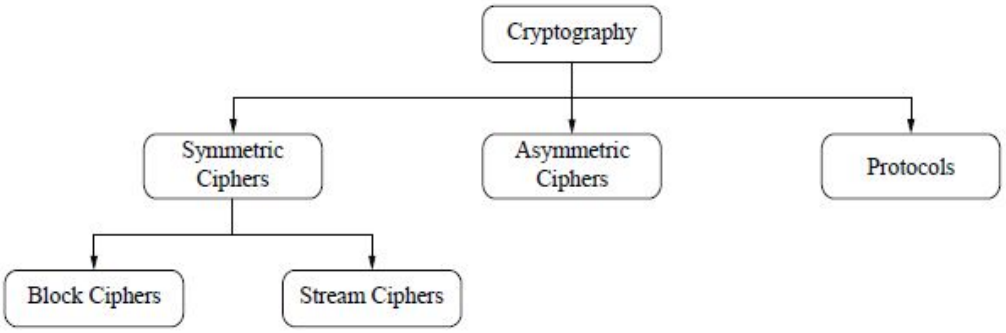



Figure 1.2: Classification of Cryptography

crypt a complete block of bits at a time. Figure 1.3 illustrates encryption using stream cipher and block cipher.

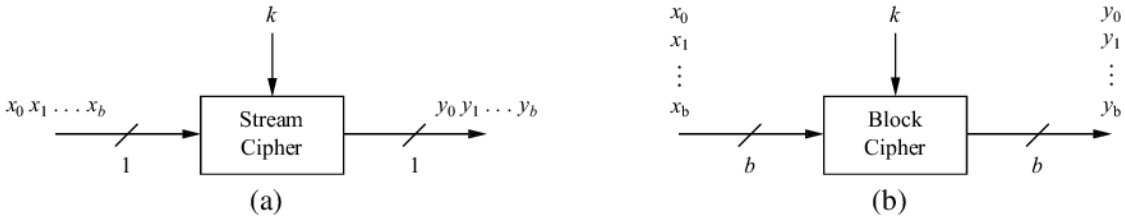



Figure 1.3: Encrypting data using Stream Cipher and Block Cipher

Block ciphers encrypt a block of bits at a time. This has a very important implication: the encryption of a plaintext bit is influenced by the other plaintext bits present in the same block. Block ciphers use the same transformation so the output is determininstic. It means that for a given input (plaintext), the output (ciphertext) will always be same. However, in case of stream ciphers, output is not deterministic because of the element of randomness involved in them.

In the field of information security, block ciphers are used more often compared to stream ciphers. As stream ciphers are small and fast, they are preferred for applications with little computational requirements like smartphones and smart cards. Modern block ciphers are very efficient in software implementation as well as hardware implementation. DES, 3DES and AES are some prime examples of block ciphers.

# CHAPTER 2

# History

Famous information theorist Claude Shannon introduced 2 primitive operations to build strong encryption algorithms: confusion and diffusion. **Confusion** means that the relationship between ciphertext and key is obscured. Substitution tables implement confusion operation. Diffusion means that one plaintext symbol influences many ciphertext symbols. **Diffusion** ensures that the statistical properties of plaintext remain obscured. Permutations implement diffusion operation. Ciphers which implement only confusion are not secure. **Substitution ciphers** and **Enigma machines** used during World War II were easily broken because they implemented confusion only. In a similar manner, ciphers which perform diffusion only are also not secure.

In 1949, Shannon proposed the concept of product cipher [1] which used combination of confusion (substitution tables) and diffusion (permutations). Afterwards, Feistel networks were introduced which used iterated product ciphers to carry out encryption in multiple rounds. Figure 2.1 shows a typical Feistel network. Each round used a different subkey derived from the original key. Feistel networks form the basis of many, but not all, modern block ciphers. DES (Data Encryption Standard) cipher is based on Feistel network whereas AES (Advanced Encryption Standard) is not a Feistel cipher. Apart from the increased cryptographic strength, Feistel networks have one very important advantage: encryption and decryption are essentially the same operation with reversed key schedule. This helps significantly in hardware and software implementations.

In 1972, NIST (National Institute of Standards and Technology) invited proposals for a standard cipher in USA. In 1974, a team of cryptographers working at IBM submitted the most promising candidate. It was an algorithm based on **Lucifer** [2] cipher. Lucifer was a Feistel cipher developed by Horst Feistel in late 1960s. NSA (National Security Agency) suggested some changes to the submitted cipher and the resulting modified cipher was DES. In 1977, NIST released DES for general public.

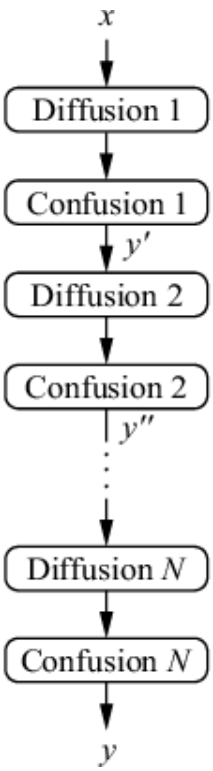



Figure 2.1: Feistel network

DES continued as the standard cipher until 1998. During that period, almost 80 percent applications used DES cipher. In 1998, a hardware machine named **Deep Crack** was developed which used brute force attack to break DES within 56 hours.

Henceforth, the use of DES became limited to applications where short term security, say few hours, is needed. Afterwards, many variants of DES emerged: 2DES, 3DES etc. In 1999, NIST announced that use of DES should be limited to legacy applications and instead 3DES should be used. Even though 3DES resisted brute force attacks, there were few problems associated with it most notably it being 3 times slower compared to DES. Moreover, with advancements in the field of quantum computing, a brute force attack on 3DES was not ruled out in upcoming future. All this led to the conclusion that a new block cipher was needed.

NIST invited proposals for a new block cipher. 15 candidate algorithms were submitted by researchers all around the globe. In August 1999, NIST narrowed down to 5 candidates: Mars(IBM), RC6(RSA Labs), Rijndael, Serpent and Twofish. The advantages and limitations of these 5 algorithms were discussed by scientific community. In 2001, NIST declared Rijndael as the AES (Advanced Encryption Standard) and published it.

# CHAPTER 3

# Structure and Working of Block Ciphers

The structure and working of famous block ciphers DES, 3DES and AES is discussed in this chapter.

## 3.1 Data Encryption Standard (DES)

DES is a symmetric cipher which means that it uses the same key for encryption as well as decryption. DES is based on Feistel network and uses an iterative algorithm. DES is a block cipher which encrypts a block of 64 bits. The size of key used in DES is 56 bits. There are 16 rounds in DES and all of them perform identical operation. Figure 3.1 and 3.2 show DES Cipher and its block diagram.

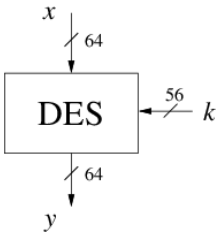



Figure 3.1: DES Cipher

First of all, a bitwise permutation IP is performed and after that the plaintext is divided into two 32 bit sub-blocks $L_0$ and $R_0$. Feistel network takes these 2 sub-blocks as input. The function f takes the right sub-block $R_i$ as input and its output is XORed with left sub-block $L_i$.

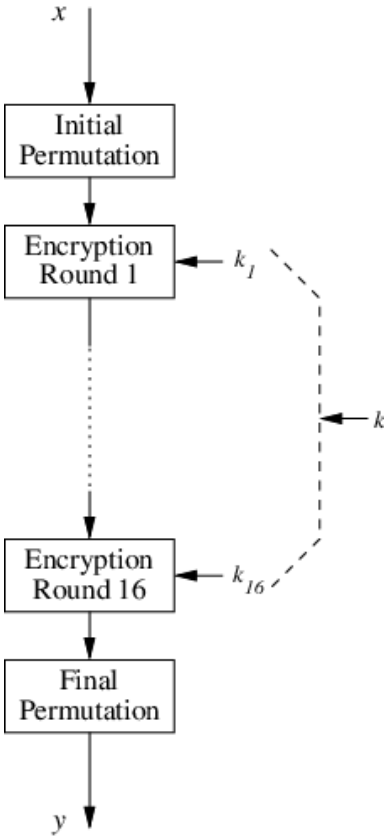



Figure 3.2: Block diagram of DES

After that, the left and right sub-blocks are swapped. This procedure keeps on repeating in the subsequent rounds and is given as:

$$L_i = R_{i-1},$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

where i denote the round number and can be any integer from 1-16. When $16^{th}$ round ends, the two 32 bit sub-blocks $L_{16}$ and $R_{16}$ are re-swapped. Lastly, the final permutation $IP^{-1}$ is performed. $IP^{-1}$ and IP are inverse of each other. Each round i uses a 48 bit sub-key $k_i$ derived from original 56 bit key k. Figure 3.3 summarizes the Feistel structure of DES.

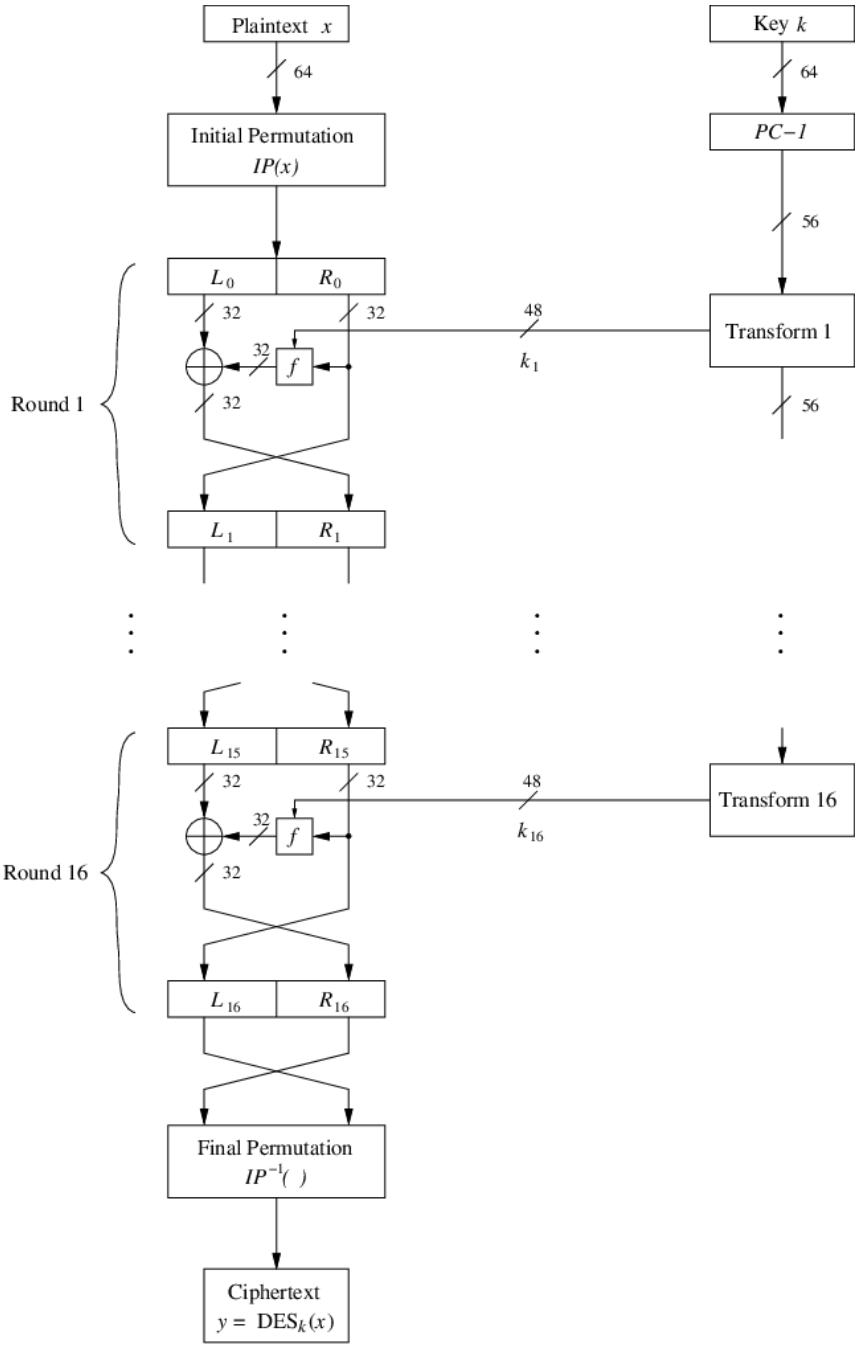



Figure 3.3: Feistel structure of DES

### 3.1.1 Initial and Final Permutations

These 2 are bit-wise permutations. These are easy to implement in hardware but are relatively slow in software. Both these permutations do not contribute to security of DES.

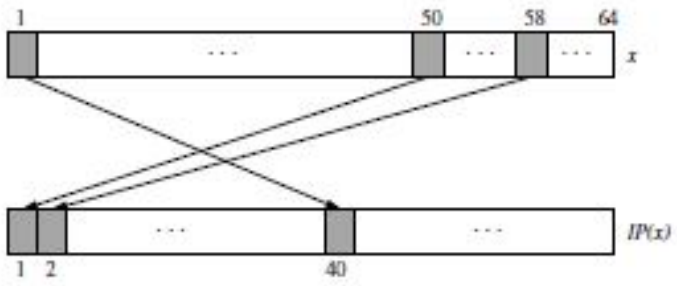



Figure 3.4: Initial Permutation

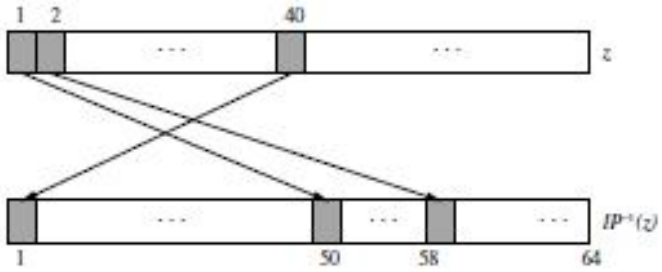



Figure 3.5: Final Permutation

### 3.1.2 The Function f

It plays a very important role in security of DES. In $i^{th}$ round, the right sub-block $R_{i-1}$ of preceding round and sub-key $k_i$ serve as input to the function f. Its output is XORed with left sub-block $L_{i-1}$ of preceding round. Figure 3.6 shows the block diagram of function f.

E-box (Expansion box) is a unique permutation. As it can be clearly seen from block diagram, the E-box expands the 32 bit input to 48 bits. This is achieved as follows: firstly the 32 bit input is divided into 8 blocks of 4 bit each and then each of these 4 bit block is expanded to 6 bits. Out of the 32 input bits, 16 bits are used once in the output and 16 are used twice. Figure 3.7 shows how expansion works.

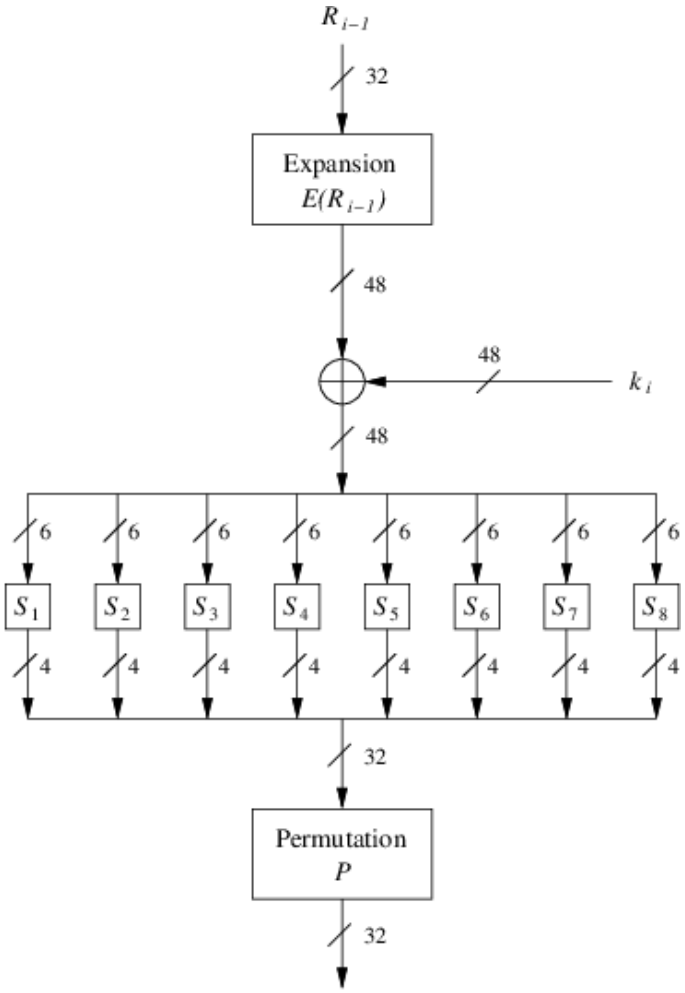



Figure 3.6: Block diagram of function f

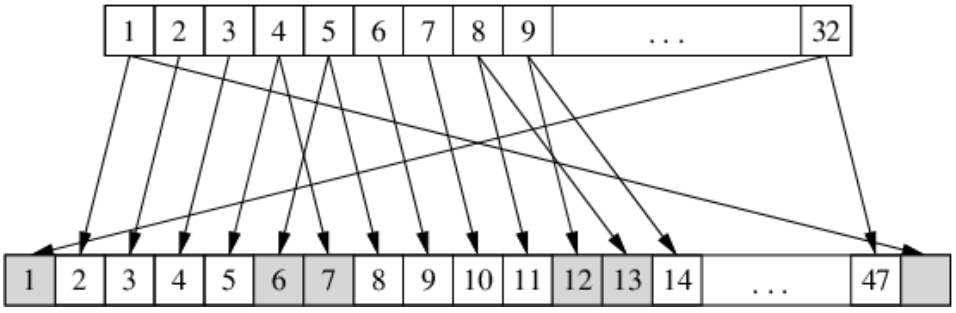



Figure 3.7: Working of expansion

After that XOR operation is performed between the 48 bit output of E-box and the round key $k_i$. The resulting 48 bits are divided into 8 blocks of 6 bit each. These 6 bit blocks serve as input to 8 different S-boxes (Substitution boxes). S-box is a table which maps input of 6 bits to output of 4 bits. There are $2^6 = 64$ entries in every S-box and size of each entry is 4 bits. The 64 entries of the S-box are arranged in a table of 4 rows and 16 columns. The decimal value obtained by combining MSB and LSB of 6 bit input gives the row number of the table whereas column number is obtained from the decimal value of remaining 4 bits. A typical S-box is shown in Figure 3.8 where the integer entry is the decimal value of 4 bit output.

| $S_1$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| 1 | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 01 | 10 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| 2 | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| 3 | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

Figure 3.8: S-box $S_1$

The S-boxes provide non-linearity to DES, i.e., $S(a) \oplus S(b) \neq S(a \oplus b)$.

Lastly, output of 32 bits is fed to permutation P in which bit-wise permutation takes place. The permutation P is different from IP and $IP^{-1}$ in the sense that P contributes to the security of DES. It provides diffusion in such a way that after $5^{th}$ round each output bit is influenced by each and every bit of plain text and key. This phenomenon is termed as **Avalanche Effect**.

## 3.2 Triple DES (3DES)

After the limitations of DES were dicovered, 2DES was introduced. It used 2 consecutive encryptions using DES. However it suffered from meet in the middle attack. So 3DES was introduced.

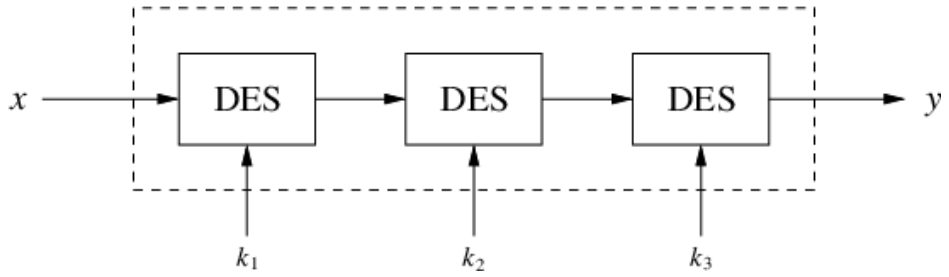



Figure 3.9: Triple DES (3DES)

3DES is based on 3 consecutive encryptions using DES with different keys.

$$y = DES_{k_3}\ (DES_{k_2}\ (DES_{k_1}\ (x)))$$

Another version of 3DES is

$$y = DES_{k_3}\ (DES^{-1}{}_{k_2}\ (DES_{k_1}\ (x)))$$

When all the keys are equal, i.e. $k_1 = k_2 = k_3$, this version resembles DES because $DES^{-1}$ nullifies one DES and only one DES encryption remains. Hence, this version helps in applications where DES is still in use.

## 3.3 Advanced Encryption Standard (AES)

AES originated from **Rijndael** block cipher. The main difference between Rijndael and AES cipher is that Rijndael can encrypt a block of 128, 192 or 256 bits whereas AES is restricted to encrypt blocks of 128 bits. In both the ciphers, key size can be 128, 192 or 256 bits. Figure 3.10 demonstrates AES cipher.

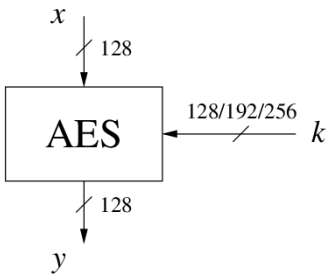



Figure 3.10: AES Cipher

The size of key decides the number of rounds in the cipher.

| **Key size** | **No. of Rounds** |
|---|---|
| 128 bits | 10 rounds |
| 192 bits | 12 rounds |
| 256 bits | 14 rounds |

AES cipher consists of 3 different layers: Byte Substitution layer (S-boxes), Diffusion layer and Key Addition layer. Diffusion layer is further divided into 2 sublayers: Shift Rows and Mix Column. Last round does not contain Mix Column sublayer so as to ensure the symmetry of encryption and decryption. Figure 3.11 gives overview of AES.

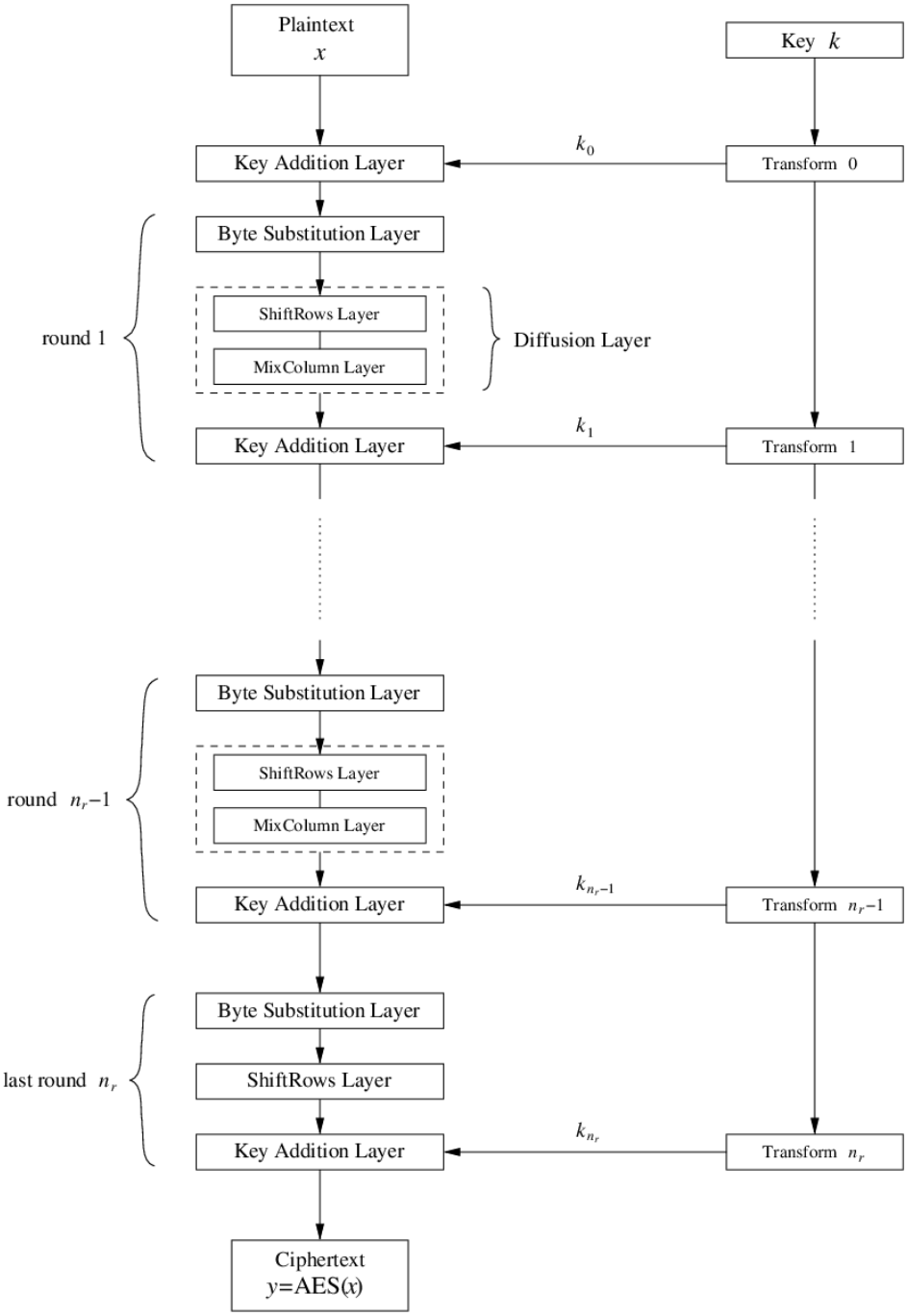



Figure 3.11: Block diagram of AES

The 128 bit block is first divided into 16 sub-blocks $A_0$, . . . ,$A_{15}$ of 1 byte (8 bits) each and is given as input to the S-boxes in a byte-wise manner. Then, byte-wise permutation is performed on the 16 byte output $B_0$, . . . ,$B_{15}$ in the Shift Rows layer. Afterwards, mixing is performed in the Mix Column layer. Finally, XOR operation is performed between the output of Mix Column layer and 128 bit subkey $k_i$ of round i. The process is summarized in Figure 3.12.

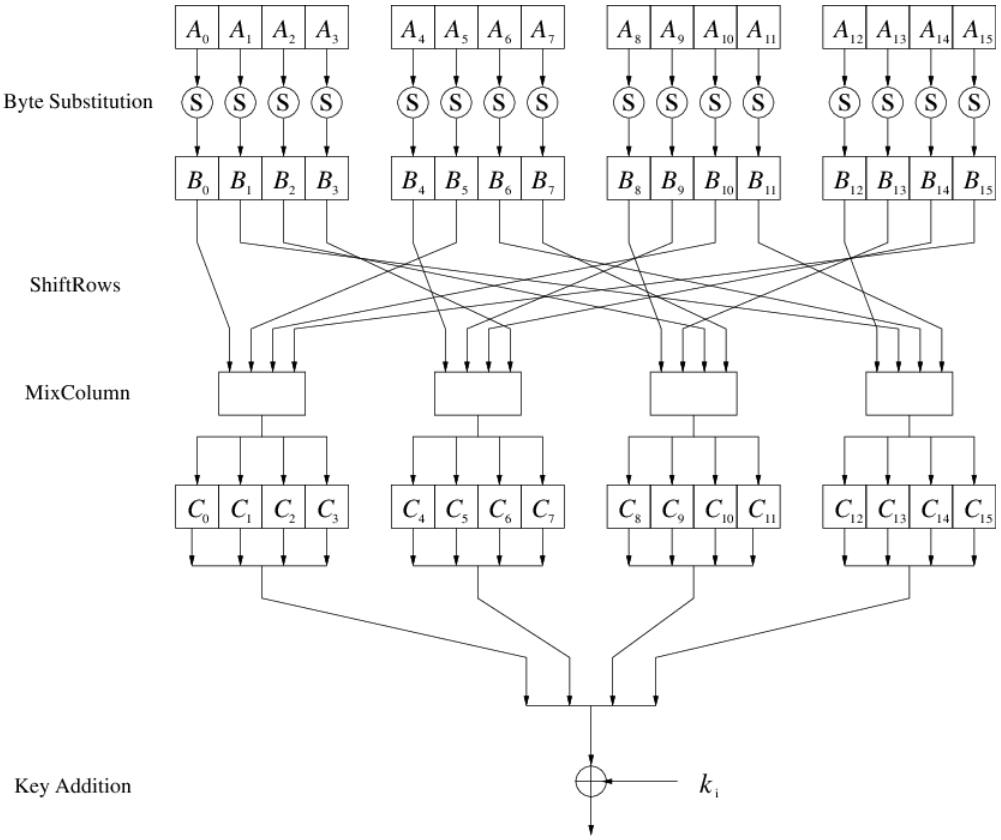



Figure 3.12: Round i of AES cipher

The sub-blocks $A_0, \ldots, A_{15}$ are arranged in a 4 by 4 matrix as follows:

| | | | |
|---|---|---|---|
| $A_0$ | $A_4$ | $A_8$ | $A_{12}$ |
| $A_1$ | $A_5$ | $A_9$ | $A_{13}$ |
| $A_2$ | $A_6$ | $A_{10}$ | $A_{14}$ |
| $A_3$ | $A_7$ | $A_{11}$ | $A_{15}$ |

Figure 3.13: 4 by 4 matrix

### 3.3.1 Byte Substitution Layer

The Byte Substitution layer consists of 16 S-boxes each with 1 byte input and output. This layer replaces each byte $A_i$ by another byte $B_i$ as:

$$S(A_i) = B_i$$

Unlike DES, all the S-boxes are identical in case of AES. S-box introduces non linearity in AES, i.e., ByteSub(A) + ByteSub(B) ≠ ByteSub(A+B). AES S-box is shown in Figure 3.14.

| | y | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| x 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

Figure 3.14: AES S-box for input byte (xy)

### 3.3.2 Shift Rows Sublayer

The matrix obtained after Byte substitution is:

| | | | |
|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ |
| $B_1$ | $B_5$ | $B_9$ | $B_{13}$ |
| $B_2$ | $B_6$ | $B_{10}$ | $B_{14}$ |
| $B_3$ | $B_7$ | $B_{11}$ | $B_{15}$ |

Figure 3.15: Before Shift Rows

The second row is shifted 1 byte to the left. The third row is shifted 2 bytes to the left. The fourth row is shifted 3 bytes to the left. The first row is kept unchanged. Shift Rows results in following matrix:

| | | | | |
|---|---|---|---|---|
| $B_0$ | $B_4$ | $B_8$ | $B_{12}$ | no shift |
| $B_5$ | $B_9$ | $B_{13}$ | $B_1$ | ⟵ one position left shift |
| $B_{10}$ | $B_{14}$ | $B_2$ | $B_6$ | ⟵ two positions left shift |
| $B_{15}$ | $B_3$ | $B_7$ | $B_{11}$ | ⟵ three positions left shift |

Figure 3.16: After Shift Rows

### 3.3.3 Mix Column Sublayer

Mix Column provides diffusion to AES by mixing the columns using a linear transformation. The 16 byte output matrix is denoted by C.

$$\text{MixColumn(B)} = \text{C}$$

Each column of C is calculated as follows:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

Figure 3.17: Mix Column operation on first column

### 3.3.4 Key Addition Layer

The output of the Mix Column layer is a 16 byte matrix C. This matrix constitutes of 128 bits which are XORed with 128 bit subkey $k_i$ to complete the round i.

## 3.4 Structural differences between DES and AES

1. DES is based on Feistel network whereas AES is not.
2. DES is bit oriented whereas AES is byte oriented.
3. All the S-boxes are different in DES whereas in case of AES, they are identical.
4. In a single round, DES encrypts only half of input (32 out of 64 bit) whereas AES encrypts the complete input (128 bit). This is the main reason why AES requires less number of rounds compared to DES.
5. In DES all the rounds are identical whereas in AES, last round is different from other rounds as it does not contain Mix Column sub-layer.
6. DES is restricted to use key size of 56 bits whereas AES can use key size of 128 bits, 192 bits or 256 bits.

# CHAPTER 4

# State of the art

This chapter discusses the current status of Block ciphers like DES, 3DES, AES etc. Ongoing research and open research problems are also discussed.

## 4.1 Current status of DES

DES has been the most popular block cipher of late 20th century. It is still resistant to analytical attacks like differential cryptanalysis [3] or linear cryptanalysis [4]. However, DES is not considered secure nowadays. Due to its small key size, it is possible to perform exhaustive key search (brute force attack) on DES. Hence, use of DES is limited to legacy applications. DES is also used in application requiring short term security (say few hours).

DES is the most studied symmetric cipher. Its Feistel structure has inspired many modern ciphers. Therefore, its study is considered very important and helps in gaining valuable insights into other modern ciphers. DES is a very important milestone in the evolution of cryptography.

## 4.2 Current status of 3DES

Although DES might have become obsolete, its variant 3DES is still very much in use. 3DES is still secure due to its large key size (168 bit). It is popular in financial applications. It is also used in electronic passwords to ensure security of biometric data.

## 4.3 Current status of AES

In modern world, AES is the most used symmetric cipher. WiFi encryption standard, TLS (Transport Layer Security), IPSec (Internet Protocol Security), SSH (Secure

Shell), Skype and many other security products use AES. It is also used to encrypt many classified documents of secret or top secret level.

## 4.4 Recent Block Ciphers

The Feistel structure of DES has inspired many modern ciphers like Mars, CAST, MISTY1, Twofish, Blowfish, RC6 etc. However, not all modern ciphers are based on DES. A recent cipher IDEA [5] is pretty much different from DES. Its basic operations involve use of arithmetic on 3 different algebraic components.

Lightweight ciphers are gaining importance due to the advent of smartphones and smart cards. They are also needed when huge volumes of data has to be encrypted and time complexity is quite high if we use traditional ciphers. PRESENT [6], mCrypton [7] and HIGHT [8] are few examples of lightweight ciphers.

## 4.5 Ongoing Research

Currently, there are many open reasearch areas in the field of block ciphers. Some prominent ones are given below:

### 4.5.1 Cryptanalysis of AES and similar block ciphers

First of all, research is being conducted to establish proof that AES is secure against analytical attacks like differential cryptanalysis and linear cryptanalysis. Also, researchers are investigating and trying to discover attacks which can exploit the algebraic structures which make up the AES cipher. Moreover, a recent trend in this area is to use the system of quadratic equations to recover the key.

### 4.5.2 Construction of new block ciphers

Researchers aim to develop new block ciphers which use lesser number of gates, encrypt larger blocks, have fast key setup and have improved efficiency and security. An alternative of AES named KASUMI is being used in smartphones due to its low gate count.

### 4.5.3 Generic tradeoff attacks

The time-memory-data attack which is used against stream ciphers is being investigated to exploit block ciphers.

## 4.6 Open Research Problems

Few open research problems in the field of block ciphers are given below:

1. Construction of an efficient block cipher whose security can be proved to be directly related to unsolvability of a well known and studied problem of mathematics.
2. Determining alternate strategies to construct block ciphers as most of the current ciphers are based on Feistel networks, S-boxes etc. [9]
3. Estimating the optimal number of rounds for ciphers which operate iteratively. We use 16 rounds in DES and 10/12/14 rounds in AES because their proposers said so. There is a need to find the number of rounds which provide best security.
4. Developing attacks which are not influenced by the no. of rounds.
5. Stating optimal properties for an S-box in order to improve efficiency and security.

# CHAPTER 5

# Limitations and Attacks

This chapter discusses limitations and attacks related to block ciphers DES, 3DES and AES.

## 5.1 Limitations and Attacks related to DES

DES is resistant to **analytical attacks**. In order to perform **differential cryptanalysis** on DES, $2^{47}$ known pairs (x,y) of plaintext x and ciphertext y are needed. It is highly impractical to obtain such a large number of pairs. Similarly, **linear cryptanalysis** on DES requires $2^{43}$ pairs of plaintext and ciphertext which is again an impractical number.

DES has a significant limitation because of its **small key size (56 bit only)**. With the advancements going on in the field of quantum computing, it has become quite easy to break DES by performing an **exhaustive key search (bruteforce attack)**.

## 5.2 Limitations and Attacks related to 3DES

Similar to DES, 3DES is also resistant to analytical attacks like differential cryptanalysis and linear cryptanalysis. As it uses a key size of 168 bit it is also resistant to any bruteforce attack imaginable at this moment. However, with advancements in the field of technology, a **bruteforce attack** is not ruled out in future. 3DES has its own limitations. Since it uses DES 3 times in a sequential manner, it is **3 times slower** compared to DES. It is very efficient when implemented in hardware but not so in software. Also it can encrypt a **short block of 64 bit** at a time. Hence, if we want to encrypt huge volumes of data, use of 3DES will result in very high time complexity.

## 5.3 Limitations and Attacks related to AES

Till date, not a single attack, against AES, has been discovered which is better than brute force attack [10]. On AES, brute force attack itself is tedious because AES can use a **key size as large as 256 bits**. The only limitation associated with AES is that it is restricted to encrypt **blocks of size 128 bits only**. With other modern ciphers encrypting blocks of size upto 256 bits, AES lags behind them in this respect.

# CHAPTER 6

# Conclusion

Block ciphers are one of the most important crytographic tools available in modern world. Modern day cryptography owes a lot to the introduction of block ciphers like DES. In fact, DES and attempts to break it triggered the growth of cryptography. Although, DES has become obsolete nowadays (apart from legacy applications and applications requiring short term security of few hours), it is still very important. Since many modern day ciphers like Blowfish, RC6 etc are based on Feistel structure of DES, study of DES is very important. As a matter of fact, DES is the most studied symmetric cipher in the field of cryptography and information security.

Gradually, many variants of DES came into existence. Some of them like 2DES are irrelevant today while some like 3DES are still in use. 3DES is used mainly in financial applications and in electronic passports. However, with rapid advancements in the field of technology, these traditional ciphers will lose their relevance. AES was introduced to replace DES. It is the most used block cipher currently, finding use in WiFi Encryption Standard, Transport Level Security, Skype etc. At the moment, there is no practical attack against AES and it is expected to be like this in upcoming years.

With the advent of smartphones, smart cards and many other embedded applications, lightweight ciphers are gaining importance. Research is being carried out in the area of lightweight ciphers. PRESENT is an important lightweight block cipher. Hence, we can conclude that block ciphers are one of the most important foundation on which the branch of cryptography was built and is evolving continuously.

# REFERENCES


[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. Sorkin, "Lucifer, a cryptographic algorithm," *Cryptologia*, vol. 8, no. 1, pp. 22–42, 1984.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.

[4] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Annual International Cryptology Conference*, pp. 1–11, Springer, 1994.

[5] H. Lipmaa, "Idea: A cipher for multimedia architectures?," in *International Workshop on Selected Areas in Cryptography*, pp. 248–263, Springer, 1998.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *International workshop on cryptographic hardware and embedded systems*, pp. 450–466, Springer, 2007.

[7] C. H. Lim and T. Korkishko, "mcrypton–a lightweight block cipher for security of low-cost rfid tags and sensors," in *International Workshop on Information Security Applications*, pp. 243–258, Springer, 2005.

[8] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, *et al.*, "Hight: A new block cipher suitable for low-resource device," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 46–59, Springer, 2006.

[9] A. Canteaut, D. Augot, C. Cid, H. Englund, H. Gilbert, M. Hell, T. Johansson, M. Parker, T. Pornin, B. Preneel, M. Robshaw, and C. Rechberger, "D.stvl.9 - ongoing research areas in symmetric cryptography," 01 2008.

[10] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.