

Names: Yasar Azimi

ID:# 44158

Assignment 3

Dr.Abdalrahman Alfagi

Class: ITC 370

2023/11/28

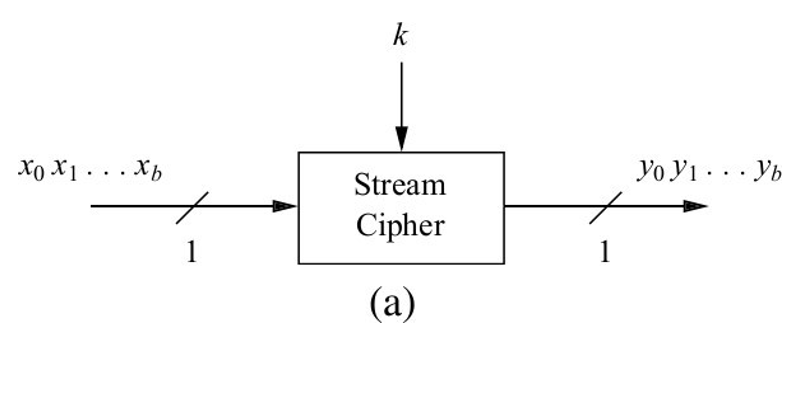
**Introduction**:

In cryptography, modern encryption methods are playing an important role in securing information whether they are for sending messages, applications, website’s or games. Two fundamental types of encryption schemes are stream ciphers and block ciphers. In this report, we will explore the concepts of stream ciphers and block ciphers, delve into the structure of the Feistel cipher, examine the Data Encryption Standard (DES), and discuss the Advanced Encryption Standard (AES).

**Main** **Body**:

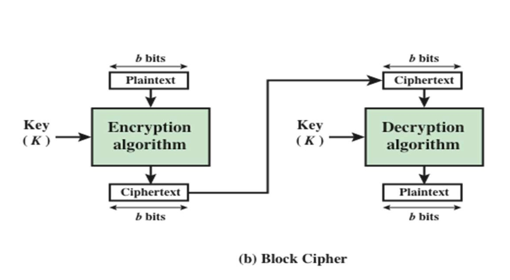
* 1. **Stream Cipher:**

Stream ciphers process messages a bit or byte at a time when encrypting or decrypting. They were invented in 1917 by Gilbert Vernam, who is known for the creation of the one-time pad technique. Stream ciphers process data sequentially, and encryption involves adding a truly random key bit by bit, commonly denoted by XOR. The best example would be: one time Pad cipher…



**1.2 Block Cipher:**

A block cipher is an encryption/decryption scheme where a block of plaintext is treated as a whole to produce a cipher text block of equal length. It is applicable to a broader range of applications than stream ciphers. Block ciphers operate on fixed-size blocks (e.g., 64 or 128 bits), and various modes of operation determine their use in different scenarios. They are used in broader range than stream cipher while there are 2 ^ N (2 to power n) encryption block for it to be reversed. The best example would be: DES…



**2. Feistel Cipher:**

A Feistel cipher is a modern substitution-transposition product cipher in a way that the end result is stronger than the components of it and it’s based on substitution-permutation (S-P) networks which was introduced by Shannon in 1949, and are the foundation of modern block ciphers. It provides confusion and diffusion to messages, for enhancing its security.

**2.1 S-P technique bases:**

S-P networks rely on two primitive cryptographic operations called: substitution (S-box) and permutation (P-box/transposition). And by combining these two, it’s capable of achieving confusion and diffusion. The practical application involves uniquely replacing plaintext elements (Substitution) and changing the order of elements (Permutation). Shannon's approach ensures complexity and security in the relationship between cipher text and the key, making it resistant to attacks.

1. **Substitution:**

Involve uniquely replacing each plaintext element or group with corresponding cipher text elements or groups.

1. **Permutation:**

Involves changing the order of elements in the sequence without adding, deleting, or replacing them.

1. **Confusion:**

Makesthe relationship between cipher text and the key as complex as possible. It ensures that the cipher text give no clue about the plaintext, which is achieved through substitution techniques.

1. **Diffusion:**

Involves increasing the redundancy of plaintext by spreading it across rows and columns, achieved through permutation (transposition) techniques.

The design model of Feistel cipher was used to create different block ciphers such as: DES (Data encryption standard), AES (Advance encryption standard), and TDEA (Triple data encryption algorithm).

**The Design Principles:**

1. **Block size:**

Bigger block side means better security but slower encryption/decryption speed.

1. **Key size:**

Larger key size means better security but slower encryption/decryption speed.

1. **Number of rounds:**

The larger the number of round the more security it has.

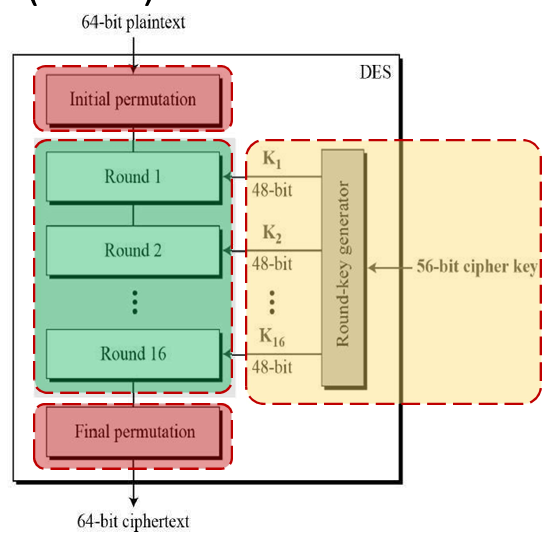
1. **Subkey generation algorithm:**

Greater the complexity of algorithm the stronger the security it has.

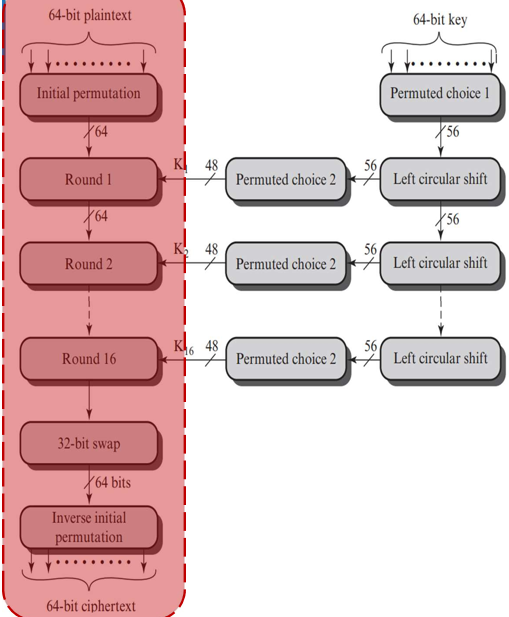
**3. DES (Data Encryption Standard):**

DES, initially issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46, is a symmetric block cipher. The algorithm is officially referred to as the Data Encryption Algorithm (DEA). And it was the most dominant symmetric encryption algorithm, until the introduction of the Advanced Encryption Standard (AES) in 2001.

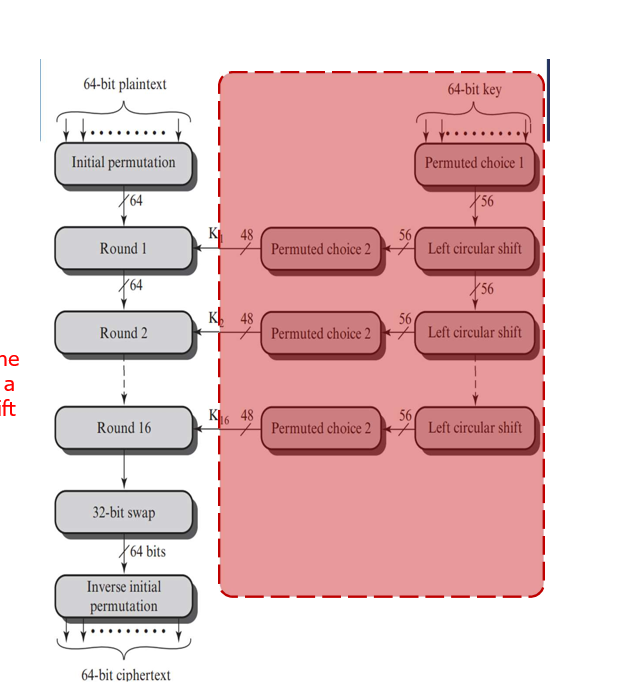
DES follows the structure of a Feistel cipher, with the exception of the initial and final permutations. And the data’s are encrypted in 64-bit blocks using a 56-bit key. The algorithm works by transforming a 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption. DES operates with a fixed key size of 56 bits, making it susceptible to modern cryptographic attacks. With the advent of AES, DES has been deemed insecure due to its small key size.



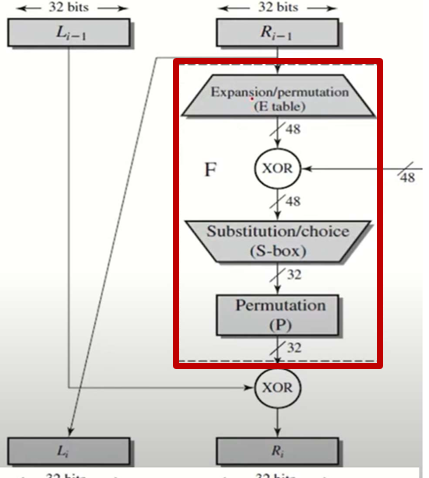
In DES block diagram we have 3 phases, 1- Initial permutation, 2- 16 rounds which involves, functions and left and right part of data, keys and its output and finally 3- the final permutation.

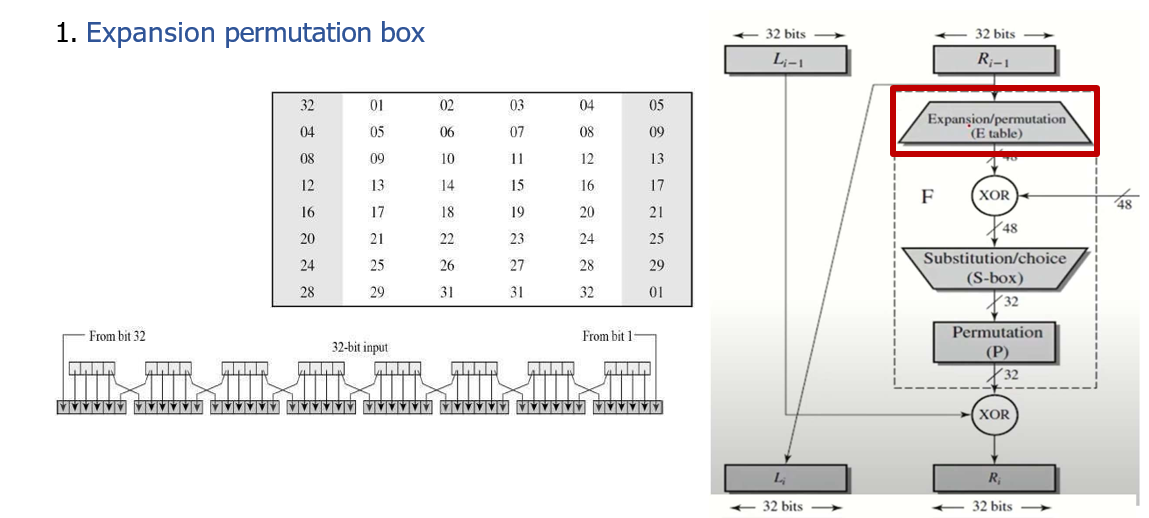


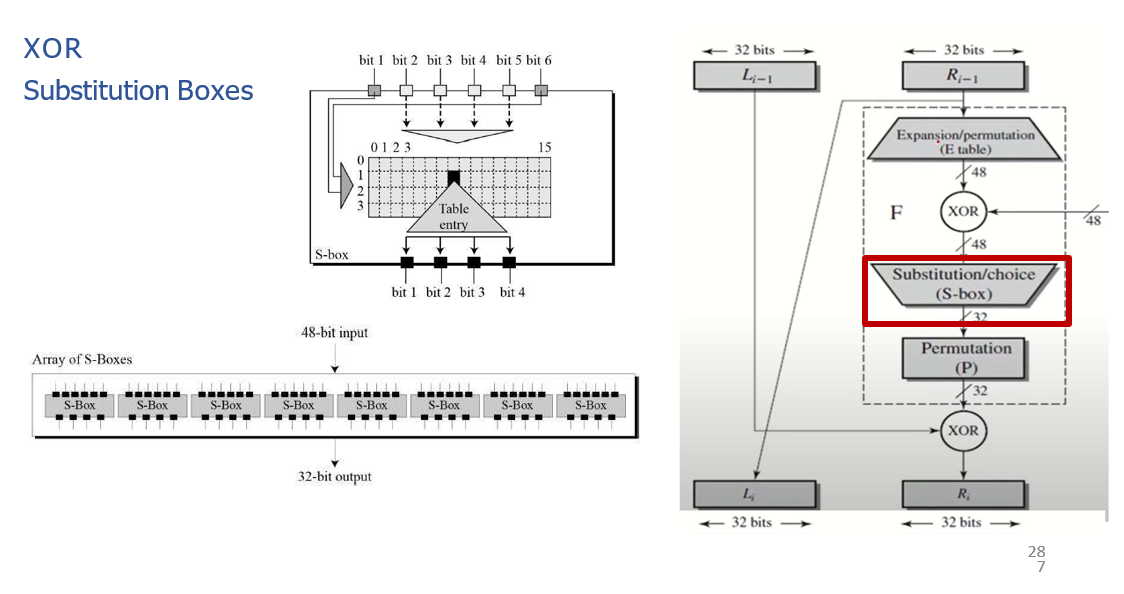
Now the key has 2 function, 1- Initial permutations and 2- 16 rounds stages involving shifts and permutation choices.



In a single around we have 1- Expansion permutation box, 2- XOR, 3- Substitution Boxes, 4- Straight permutation.



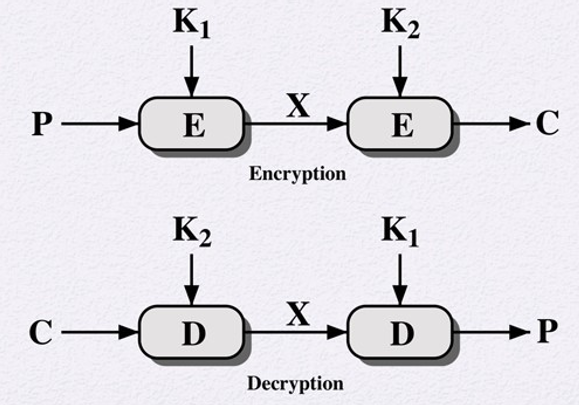




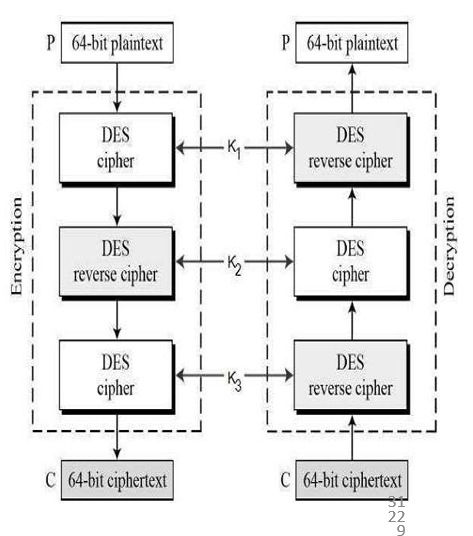
The problem with Des is that it is vulnerable to attacks with 56 bits, so until a new method could be found to replace it, other methods were purposed to strengthen the DES against such attacks and those method were:

1. **Double DES:**

Is an aversion of the data encryption system which is using the algorithm twice to the plain text but with different keys each time, so with double DES we get 2^56\*2 = 2^112 operations.

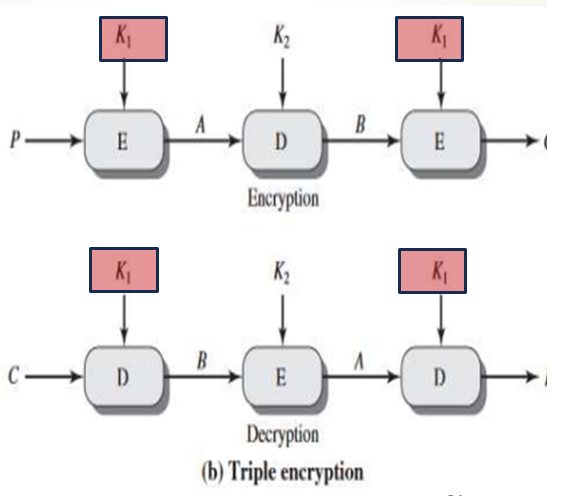


1. **Triple DES:** There are two types of Triple DES known:
2. **3 Keys Triple DES:**
3. First the plain text is encrypted with single DES using Key 1, then its decrypted using key 2, and finally it’s encrypted with single DES using key 3. And the Decryption of the cipher text is just its reverse. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.



1. **2 Keys Triple DES:**

For this we first Encrypt the plaintext using single DES with key K1, then decrypt with key K2, and finally encrypt with K1 again.



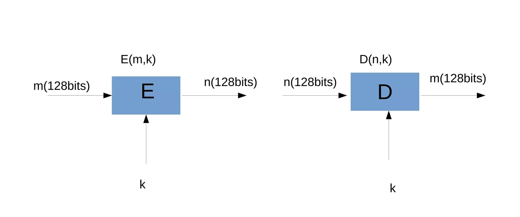
**4- AES (Advance encryption standard):**

AES, a symmetric block cipher adopted by NIST in 2001, was designed to replace DES as the approved standard for a wide range of applications. It is characterized by its complex structure and stronger security base. AES is a private key symmetric block cipher, operating on 128-bit data with key lengths of 128, 192, or 256 bits, and it is stronger and faster than Triple-DES. Its Real-world Implementation include:

1. VPNs (Virtual Private Networks)
2. Wi-Fi Security
3. Mobile Applications
4. Archive and Compression tools
5. OS System Components
6. Programming Language Libraries
7. Password Managers
8. Web Browsers.

With real-world implementations ranging from VPNs to web browsers, AES plays a vital role in securing digital communications. AES treats the 128 bits of a plaintext block as 16 bytes, allowing for efficient processing. AES encrypts messages in blocks of 128 bits and allows three different key lengths: 128, 192, and 256 bits. The number of encryption and decryption rounds varies based on the chosen key length, demonstrating the adaptability and robustness of the algorithm. The number of rounds in encryption and decryption depends on the key length:

1. 128-bit key: 10 rounds
2. 192-bit key: 12 rounds
3. 256-bit key: 14 rounds



**Conclusion:**

In the dynamic field of cryptography, the exploration of stream ciphers, block ciphers, the Feistel cipher, DES, and AES unveils a diverse spectrum of encryption techniques. Stream ciphers process data sequentially, while block ciphers operate on fixed-size blocks, offering tailored solutions for cryptographic needs. The Feistel cipher, rooted in Claude Shannon's insights, employs a sophisticated structure through substitutions and permutations, significantly influencing the evolution of modern block ciphers.

Introduced in 1977, DES played a pivotal role as a dominant symmetric block cipher, particularly in financial applications. However, its vulnerability due to a small 56-bit key size led to insecurity against contemporary cryptographic threats. The subsequent adoption of AES in 2001 marked a milestone in cryptographic standards. Operating on 128-bit data with key lengths of 128, 192, or 256 bits, AES's strength and speed surpassed Triple-DES, positioning it as a cornerstone in modern cryptographic applications. In essence, the journey through these cryptographic paradigms showcases a continuous commitment to secure information exchange, with each facet contributing to the intricate landscape of cryptographic security and adapting to the evolving digital landscape