وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

Data Encryption Standard

Class: Second

Lecturer: 2

Teaching the subject

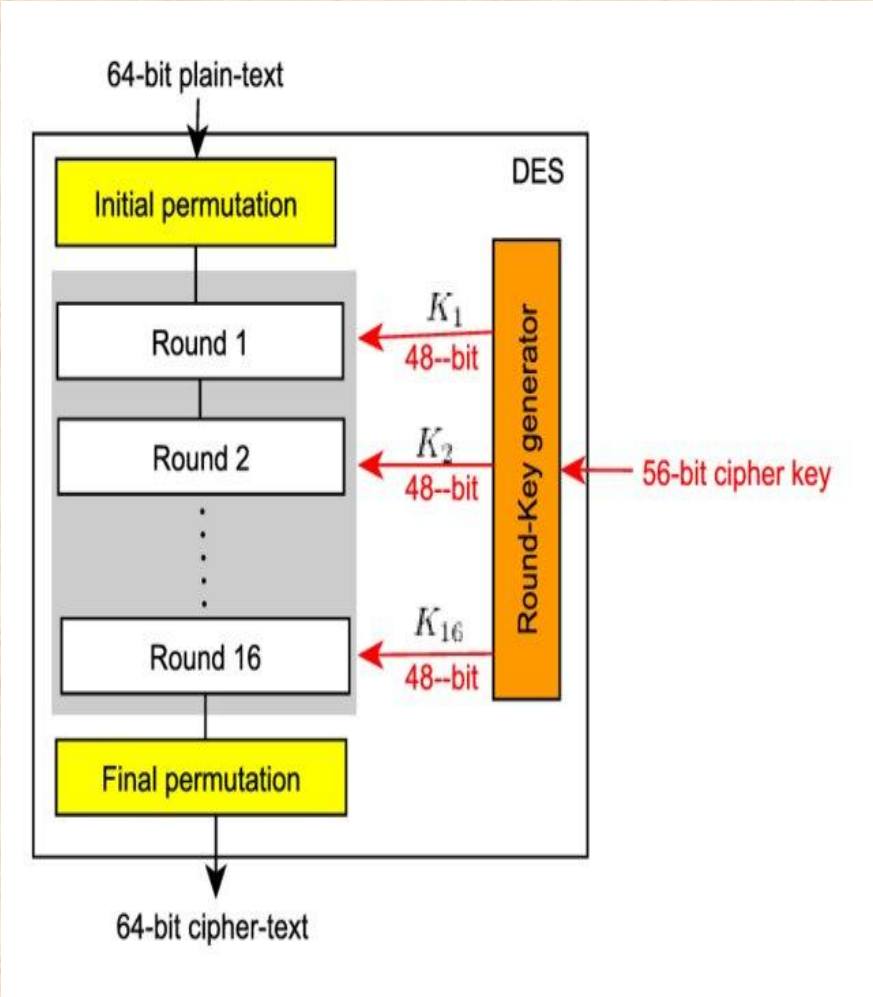
RAED ALSHMARY

Introduction

The Data Encryption Standard (DES) was developed in the early 1970s as a response to the growing need for a secure government-wide encryption standard in the United States. The National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), initiated the development of DES after consulting with the National Security Agency (NSA). IBM proposed an encryption algorithm based on Horst Feistel's Lucifer cipher, which was accepted and later standardized as DES. The algorithm became one of the most influential symmetric encryption standards in cryptographic history.

Overall Structure of DES

DES is a symmetric block cipher that encrypts data in fixed-size blocks of 64 bits using a 56-bit secret key. The algorithm consists of: An Initial Permutation (IP),16 identical rounds of processing ,A Final Permutation (FP), which is the inverse of IP.DES follows the Feistel structure, where the data block is divided into two 32-bit halves. In each round, one half is processed using a round function and combined with the other half using an XOR operation. This structure allows the same algorithm to be used for both encryption and decryption, differing only in the order of the subkeys.



Feistel Structure

The Feistel structure is a fundamental design principle of DES. It ensures that encryption and decryption are nearly identical processes. During encryption, sub keys are applied in forward order, while during decryption they are applied in reverse order. This design simplifies both hardware and software implementations and enhances efficiency.

The Feistel (F) Function

The F-function is the core of DES security. It operates on a 32-bit half-block and consists of four main stages:

a. Expansion

The 32-bit input is expanded to 48 bits using the expansion permutation (E). This step duplicates certain bits to prepare the data for key mixing.

b. Key Mixing

The expanded data is combined with a 48-bit round sub key using the XOR operation. Each round uses a different sub key derived from the main key.

c. Substitution (S-Boxes)

The result is divided into eight 6-bit blocks, each processed by a different S-box. Each S-box produces a 4-bit output using a nonlinear lookup table. The S-boxes provide nonlinearity and are the main source of DES's cryptographic strength.

d. Permutation (P-Box)

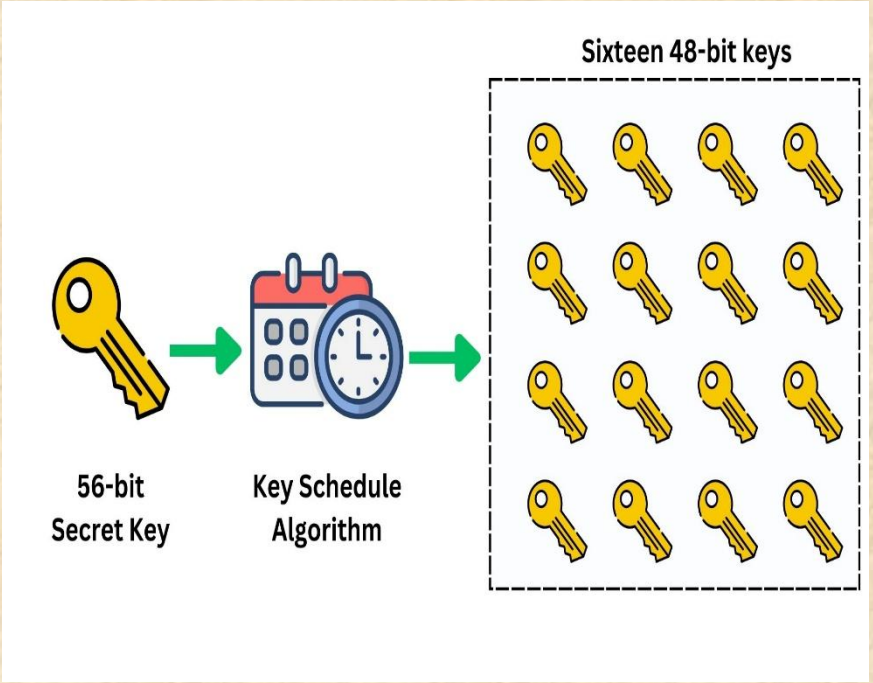
The 32-bit output from the S-boxes is permuted using a fixed permutation table. This step provides diffusion by spreading the influence of individual bits across the block.

Key Schedule

DES uses the same algorithm for both encryption and decryption. The only difference is the order of sub keys:

- Encryption uses sub keys from K1 to K16.
- Decryption uses sub keys from K16 to K1.

This property is a direct result of the Feistel structure and simplifies implementation.



Permutations in DES

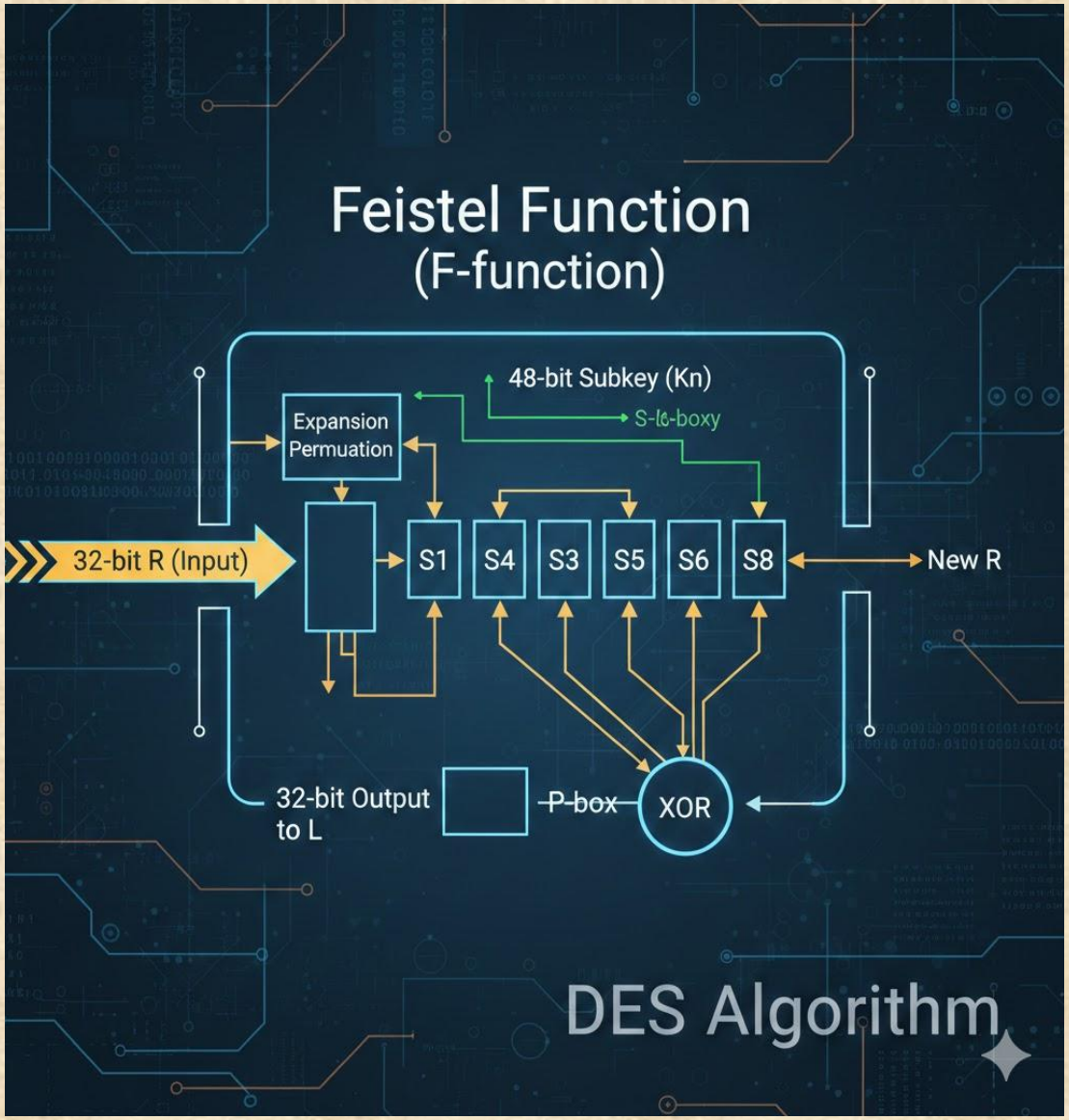
DES employs several permutations to enhance diffusion:

- **Initial Permutation (IP)** rearranges the input bits before the rounds.
- **Expansion Permutation (E)** increases the size of half-blocks.
- **P-Box Permutation** rearranges bits after substitution.
- **Final Permutation (FP)** reverses the effect of IP.

These permutations do not add secrecy by themselves but help distribute bit dependencies throughout the cipher.

S-Box Design Criteria

The S-boxes in DES were carefully designed to resist cryptanalytic attacks, particularly differential cryptanalysis. Their design criteria ensure nonlinearity, bit independence, and resistance to predictable input-output relationships. Even small changes to S-boxes can significantly weaken the security of DES.



Hardware and Software Implementations

DES has been widely implemented in both hardware and software. Hardware implementations, such as VLSI-based DES chips, achieved extremely high encryption speeds through pipelining and parallelism. Software implementations on mainframes and microprocessors also demonstrated efficient performance, making DES practical for real-world applications at the time.

Variants of DES

Several variants were developed to improve DES security:

- **Triple DES (3DES):** Applies DES three times with multiple keys to increase security.
- **DESX:** Enhances DES using whitening keys to resist brute-force attacks.
- **Generalized DES (GDES):** Uses larger block sizes but was found to be weaker under cryptanalysis.
- **DES with Alternate S-Boxes:** Modifying S-boxes or their order generally reduces security.

Security Analysis and Limitations

Despite its strong design, DES is no longer considered secure due to its short 56-bit key, which makes it vulnerable to brute-force attacks. Advances in computing power have rendered exhaustive key search feasible. Consequently, DES has been replaced by stronger algorithms such as AES.

Lecture questions

1 -What type of cryptographic algorithm is DES?
2 -What is the block size used in DES?
3 -How many rounds are used in the DES algorithm?
4 -What is the purpose of the Initial Permutation (IP)?
5 -What is the purpose of the expansion function (E)?
6 -Each S-box in DES maps?
7 -What is the main role of S-boxes?
8 -Which component generates the round subkeys?
9 -How does DES decryption differ from encryption?
10 -Which attack is DES most vulnerable to today?
11 -Which algorithm replaced DES as a standard?
12 -Which concept describes hiding relationships between key and ciphertext?
13 -DES is mainly studied today because it?

Conclusion

DES is a historically significant symmetric encryption algorithm that introduced fundamental cryptographic concepts such as the Feistel structure, confusion, and diffusion. Although it is no longer secure for modern applications, DES remains essential for understanding the foundations of modern cryptography and the evolution of encryption standards.

Scenario

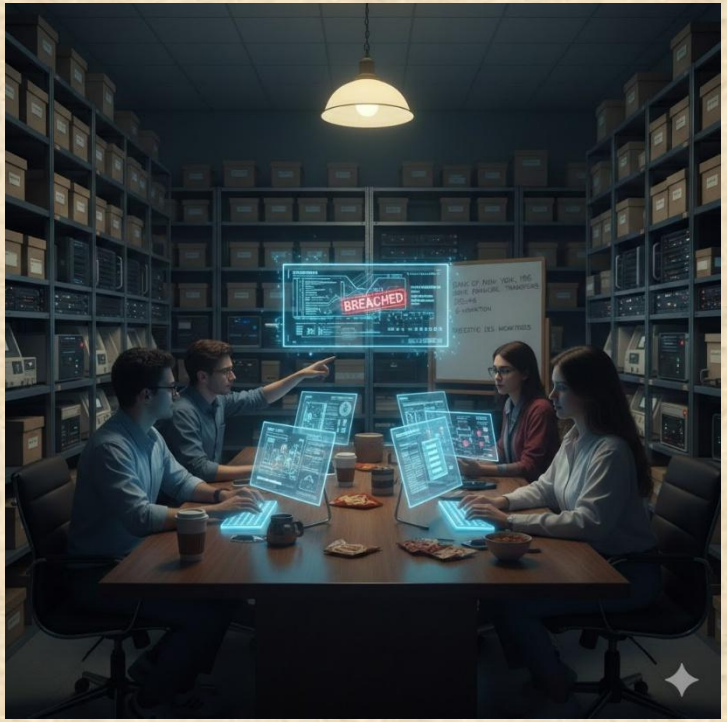
In 1995, a bank used the **Data Encryption Standard (DES)** to encrypt financial transfer data between its branches.

The system relied on a 56-bit secret key, which was updated only once every six months.

In 2026, the cybersecurity team discovered that an external entity had successfully decrypted some archived messages using advanced computing systems and brute-force attack techniques.

A team of Cyber Security students was assigned to investigate the breach and evaluate the DES structure used in the system.

1) What type of cryptographic algorithm is DES? Is it symmetric or asymmetric?
2) Why is the 56-bit key length considered a major weakness?
3) How many rounds are used in DES? What is the importance of this number?
4) How does the Feistel structure simplify encryption and decryption?
5) What is the role of the following components?
6) Why are S-Boxes considered the most critical security component in DES?
7) What type of attack was used in this scenario?
8) What alternative solutions can the team propose to secure the system today?
9) What is the difference between DES and 3DES in terms of security?
10) Why was DES replaced by AES?



Thank you