وزارة التعليم العالي والبحث العلمي

قسم علوم الامن السيبراني

Department of Cyber Security

Subject

CAST Block Cipher

Class: Second

Lecturer: 3

Teaching the subject

RAED ALSHMARY

Introduction

The **CAST Block Cipher** is a symmetric key encryption algorithm developed in Canada by Carlisle Adams and Stafford Tavares.

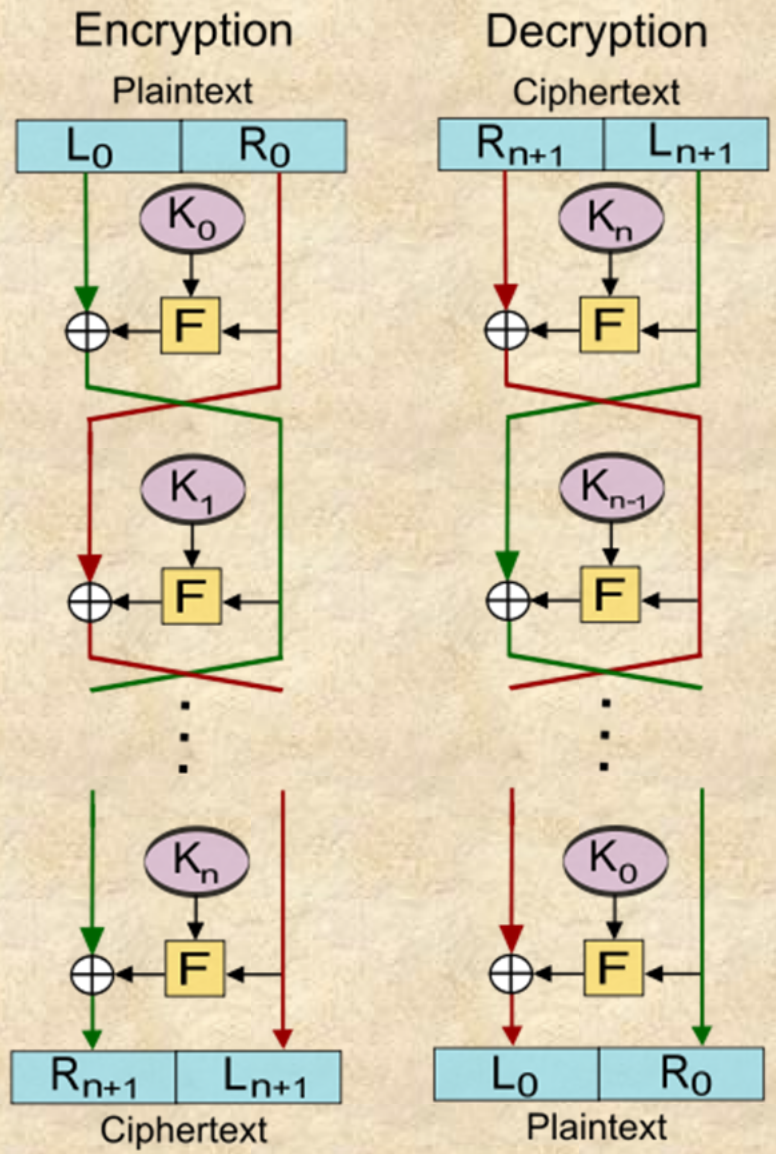
The name "CAST" is derived from the initials of its designers and also reflects the idea of achieving strong randomness and complexity in cryptographic design.

The classical version of CAST discussed in this lecture is characterized by:

- Block Size: 64 bits
- Key Size: 64 bits
- Number of Rounds: 8
- Cipher Type: Symmetric Block Cipher

General Structure

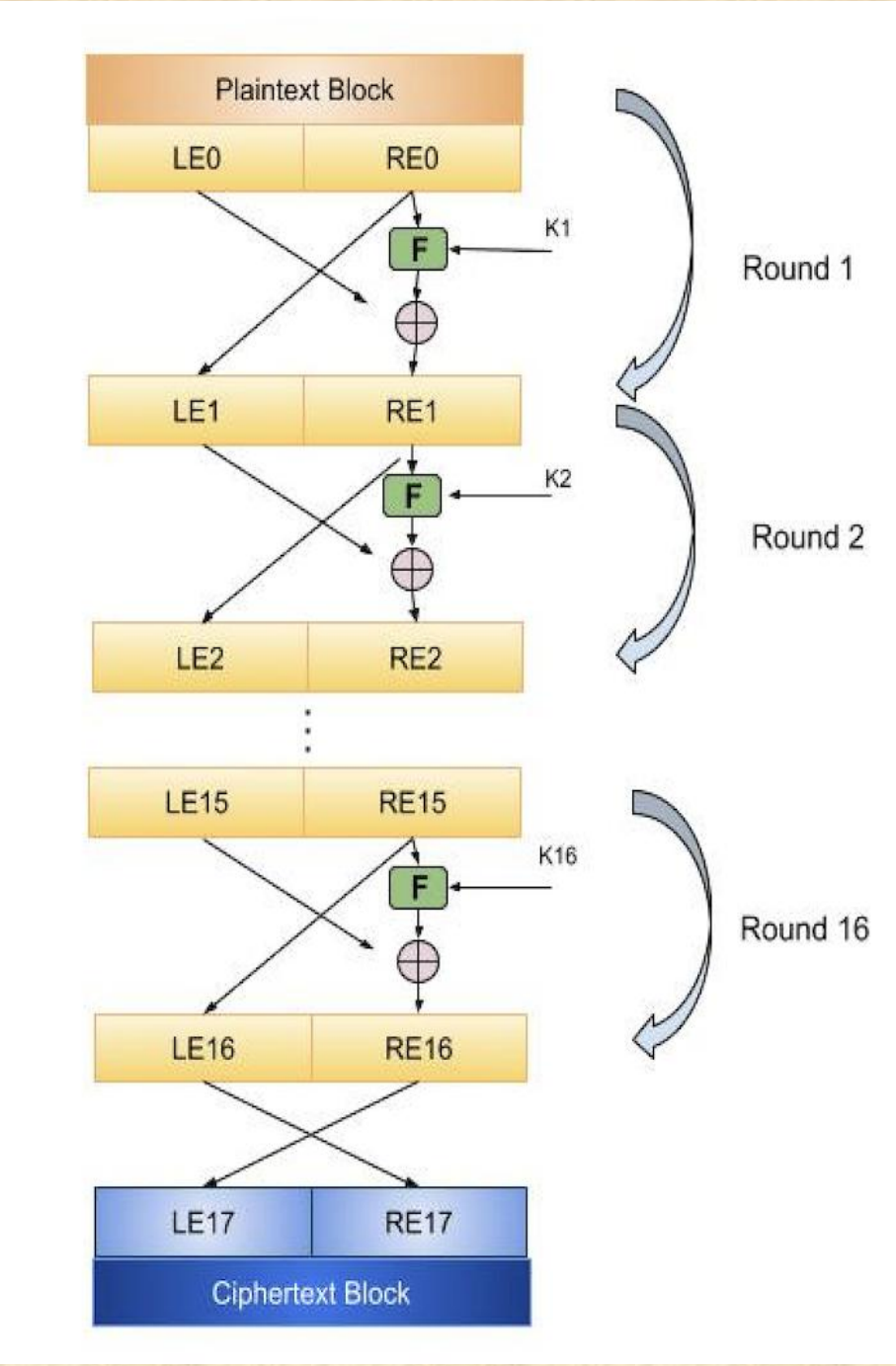
CAST is based on the Feistel Network Structure, a common design architecture in block encryption algorithms, which allows encryption and decryption to be performed using the same structure with a different order of subkeys.



Encryption Process:

1. The 64-bit plaintext block is divided into two equal halves:
   - Left half (L)
   - Right half (R)
2. The algorithm performs 8 rounds.
3. In each round:
   - The function f is applied to the right half.
   - The output is XOR ed with the left half.
   - The two halves are swapped.
4. After the eighth round, the swap is not performed.
5. The final left and right halves are concatenated to form the ciphertext.

New Right = Left ⊕ f(Right, Subkey)
New Left = Right (القديم)



Round Function (Function f)

The round function f is the core component that provides **confusion and diffusion**, two essential properties in secure encryption.

Function f Steps:

1. The 32-bit input is divided into four 8-bit segments:
   a, b, c, d
2. The 16-bit subkey is divided into two 8-bit parts:
   e, f
3. Each segment is processed through a different S-box:

Input	S-box
a	S1
b	S2
c	S3
d	S4
e	S5
f	S6

4. The six S-box outputs are XOR ed together to produce the final 32-bit output.

S-Box Design Characteristics

The strength of CAST primarily depends on its S-boxes.

Key characteristics:

- Total number: 6 S-boxes
- Input size: 8 bits
- Output size: 32 bits
- Implementation-dependent (not globally fixed)
- Not key-dependent
- Designed using strict mathematical criteria, including Bent functions
- Once selected for an implementation, they remain fixed permanently

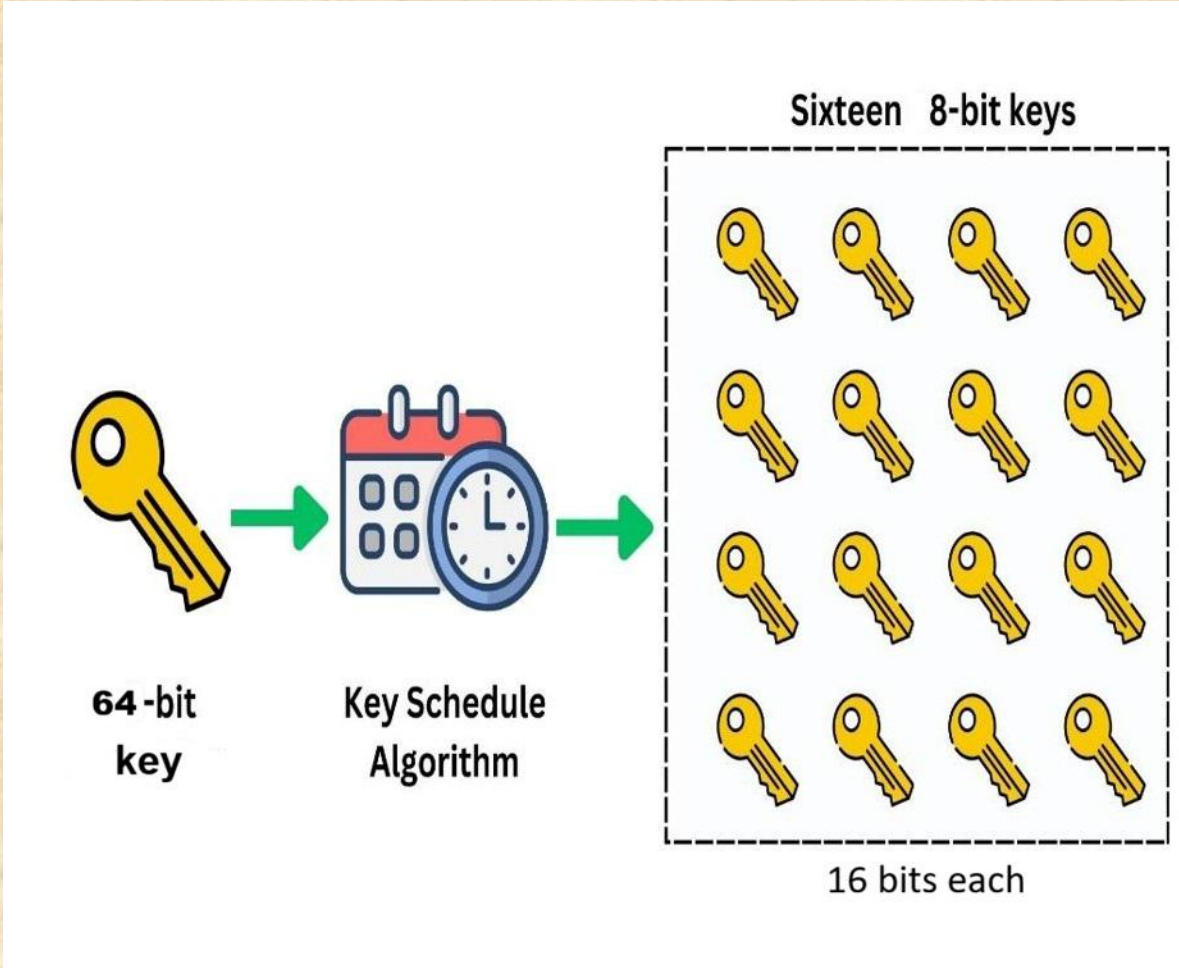
The flexibility in S-box design distinguishes CAST from algorithms such as DES.

Key Schedule

The 64-bit key is divided into 8 bytes:
k1, k2, k3, k4, k5, k6, k7, k8
Subkeys (16 bits each) are generated as follows:

Round	Subkey
1	k1, k2
2	k3, k4
3	k5, k6
4	k7, k8
5	k4, k3
6	k2, k1
7	k8, k7
8	k6, k5

This forward and reverse ordering increases structural complexity and enhances security.



Security Analysis

CAST is designed to resist:

- Differential Cryptanalysis
- Linear Cryptanalysis

Currently, there is no known practical attack against CAST other than brute-force key search.

However, since the block size is 64 bits, it may be less suitable for very large data encryption compared to modern 128-bit block ciphers.

Practical Applications

CAST has been implemented in security software such as:

- Northern Telecom
- Entrust

It was also evaluated by the Canadian government as a potential national encryption standard.

CAST, DES, and AES

CAST, DES, and AES are among the most important block cipher algorithms, playing central roles in modern cryptography.These algorithms represent three distinct phases in the design of encryption systems: strength, security, and mathematical structure.

- DES represents the classic generation of classical encryption.
- CAST represents an improved development of the Feistel architecture with flexibility in S-box design.
- AES represents the modern generation required for official read speeds.

Lecture questions

1 - 1. CAST is classified as ?
2 - CAST was developed by?
3 - The classical version of CAST uses a block size ?
4 - CAST is based on which structural design?
5 - In each round of CAST, the function f is applied ?
6 - After the final (8th) round in CAST ?
7 - The 16-bit subkey is divided into ?
8 - The strength of CAST mainly depends ?
9 - Once selected, the S-boxes in a CAST implementation ?
10 - The only known practical attack against CAST ?
11 - CAST provides confusion and diffusion mainly through ?
12 - In a Feistel structure like CAST, decryption ?

Conclusion

CAST represents an important stage in the evolution of block cipher design. It combines the classical Feistel structure with flexible and mathematically rigorous S-box construction.

Although it is not as widely adopted as modern standards like AES, CAST remains a significant academic example of secure symmetric cipher design and demonstrates strong resistance to known cryptanalytic attacks.

Thank you