قســـم الامـــــن الـــــــــسيبرانـــــــي

Department of Cyber Security

Subject:

Cast Cipher

Class:

Second

Lecturer:

Asst. lect. Mustafa Ameer Awadh

Lecture: (3)

Introduction:

CAST was designed in Canada by Carlisle Adams and Stafford Tavares. They claim that the name refers to their design procedure and should conjure up images of randomness but note the authors' initials. The example CAST algorithm uses a 64-bit block size and a 64-bit key. The structure of CAST should be familiar. The algorithm uses six S-boxes with an 8-bit input and a 32- bit output. Construction of these S-boxes is implementation-dependent and complicated. To encrypt, first divide the plaintext block into a left half and a right half. The algorithm has 8 rounds. In each round the right half is combined with some key material using function f and then XORed with **the left half to form the new right half**. The original right half (before the round) becomes the new left half. After 8 rounds (don't switch the left and right halves after the eighth round), the two halves are concatenated to form the ciphertext.

Function f is simple:

(1) Divide the 32-bit input into four 8-bit quarters: *a, b, c, d*.

(2) Divide the 16-bit subkey into two 8-bit halves: *e, f*.

(3) Process *a* through S-box 1, *b* through S-box 2, *c* through S-box 3, *d* through S-box 4, *e* through S-box 5, and *f* through S-box 6.

(4) XOR the six S-box outputs together to get the final 32-bit output.

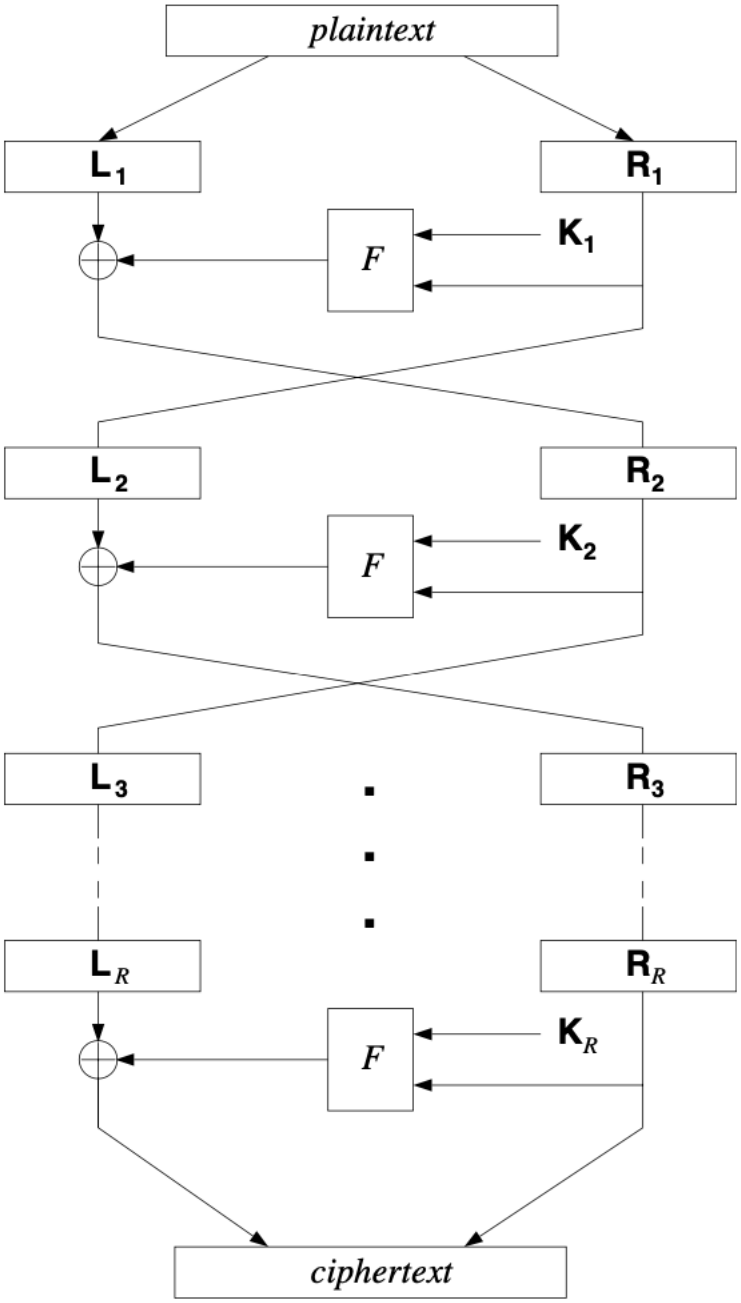

Figure 1. CAST Encryption Algorithm

Basic Characteristics of CAST

- **Block Size**: 64-bit
- **Key Size**: 64-bit
- **Number of Rounds**: 8
- **S-Boxes Used**: 6 (each with an 8-bit input and a 32-bit output)

CAST Encryption Process

1. **Divide the plaintext** into two halves:
   - **Left half (L)**
   - **Right half (R)**
2. The encryption consists of **8 rounds**.
3. In each round:
   - The right half (R) is processed using the **f function** and a subkey.
   - The result is then **XORed with the left half (L)**.
   - The original right half (R) becomes the new left half (L).
4. After 8 rounds, the two halves are concatenated to form the final **ciphertext**.
5. **No final swap** occurs after the eighth round.

The f Function

The function f is a crucial component of the CAST algorithm, ensuring security through **S-Box transformations** and **XOR operations**.

Steps of the f Function:

1. **Divide the 32-bit input into four 8-bit quarters:**
   - a, b, c, d
2. **Divide the 16-bit subkey into two 8-bit halves:**
   - e, f
3. **Process the values through S-Boxes:**
   - a → **S-Box 1**
   - b → **S-Box 2**
   - c → **S-Box 3**
   - d → **S-Box 4**
   - e → **S-Box 5**
   - f → **S-Box 6**

4. **XOR the outputs of all six S-Boxes** to produce the final **32-bit output**.

Key Features of CAST Encryption

- **Confusion and Diffusion**: Ensures that a small change in the plaintext or key results in a significant change in the ciphertext.
- **S-Box Complexity**: Uses six non-linear S-Boxes, making it resistant to linear and differential cryptanalysis.
- **Efficient Key Schedule**: Generates subkeys dynamically for each round, enhancing security.

The strength of this algorithm lies in its S-boxes. CAST does not have fixed S-boxes; new ones are constructed for each application. Design criteria are in; bent functions are the S-box columns, selected for several desirable S-box properties. Once a set of S-boxes has been constructed for a given implementation of CAST, they are fixed for all time. The S-boxes are implementation-dependent, but not key-dependent. The CAST is resistant to differential cryptanalysis, CAST is resistant to linear cryptanalysis. There is no known way to break CAST other than brute force. Northern Telecom is using CAST in their Entrust security software package for Macintoshes, PCs, and UNIX workstations. The S-boxes they chose are not public. The Canadian government is evaluating CAST as a new encryption standard. CAST is patent pending.