Symmetric Key Ciphers

Debdeep Mukhopadhyay

Assistant Professor

Department of Computer Science and Engineering

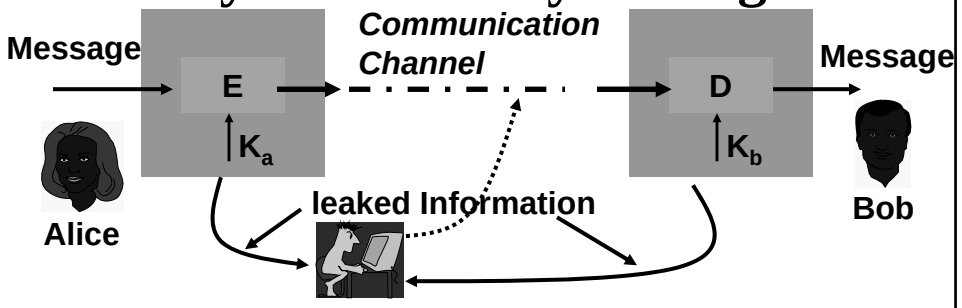
Indian Institute of Technology Kharagpur

INDIA -721302

Objectives

- Definition of Symmetric Types of Symmetric Key ciphers
  - Modern Block Ciphers
- Components of a Modern Block Cipher
  - PBox (Permutation Box)
  - SBox (Substitution Box)
  - Swap
  - Properties of the Exclusive OR operation
- Diffusion and Confusion
- Types of Block Ciphers
- The DES Cipher

Symmetric Key Setting



Assumptions

K_a is the encryption key, K_b is the decryption key.

For symmetric key ciphers, $K_a=K_b$

- Only Alice and Bob knows K_a (or K_b)

- Eve has access to E, D and the Communication Channel but does not know the key K_a (or K_b)

Types of symmetric key ciphers

- Block Ciphers: Symmetric key ciphers, where a block of data is encrypted
- Stream Ciphers: Symmetric key ciphers, where block size=1

Block Cipher

- A symmetric key modern cipher encrypts an n bit block of plaintext or decrypts an b bit block of ciphertext.
- Padding:
  - If the message has fewer than n bits, padding must be done to make it n bits.
  - If the message size is not a multiple of n, then it should be divided into n bit blocks and the last block should be padded.

Components of a Modern Block Cipher

- Most important components:
  - PBox: It is a key-less fixed transposition cipher
  - SBox: It is a key-less fixed substitution cipher
- They are used to provide:
  - **Diffusion:** it hides the relationship between the ciphertext and the plaintext
  - **Confusion:** it hides the relationship between the ciphertext and the key

Principle of Confusion and Diffusion

- The design principles of Block Cipher depends on these properties
- The S-Box is used to provide **confusion**, as it is dependent on the unknown key
- The P-Box is fixed, and there is no confusion due to it
- But it provides **diffusion**
- Properly combining these is necessary.

Diffusion (P) Boxes

- Straight Boxes

Example 24x24 Box

01	**15**	**02**	**13**	**06**	**17**	**03**	**19**	**09**	**04**	**21**	**11**
14	**05**	**12**	**16**	**18**	**07**	**24**	**10**	**23**	**08**	**22**	**20**

- Expansion Boxes

Example 12x24 Box

01	**03**	**02**	**01**	**06**	**17**	**03**	**07**	**09**	**04**	**09**	**11**
02	**05**	**12**	**04**	**06**	**07**	**12**	**10**	**11**	**08**	**10**	**08**

- Compression Boxes

Example 24x12 Box

01	**15**	**02**	**13**	**06**	**17**	**03**	**19**	**09**	**04**	**21**	**11**

SBox

An SBox (substitution box) is an mxn substitution box, where m and n are not necessarily same.

Each output bit is a Boolean function of the inputs.

$$y_1 = f_1(x_1, x_2, ..., x_n)$$
$$y_2 = f_2(x_1, x_2, ..., x_n)$$
$$...$$
$$y_m = f_m(x_1, x_2, ..., x_n)$$

Non-linear SBox

$$y_1 = a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n$$
$$y_2 = a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n$$
$$...$$
$$y_m = a_{m1}x_1 \oplus a_{m2}x_2 \oplus ... \oplus a_{mn}x_n$$

In a non-linear S-Box, each of the elements cannot be expressed as above.

Eg.

$$y_1 = (x_1)^3 + x_2, y_2 = (x_1)^2 + x_1x_2 + x_3$$

Other Components

- Circular Shift:
  - It shifts each bit in an n-bit word k positions to the left. The leftmost k bits become the rightmost bits.
  - Invertible Transformation
- Swap:
  - A special type of shift operation where k=n/2
- Other operations involve split and combine.
- An important component is exclusive-or operation

Properties of Exor

Ex-or is a binary operator, which results in 1 when both the inputs have a different logic. Otherwise, it computes 0.

Symbol: $\oplus$

Closure: Result of exoring two n bit numbers is also n bits.

Associativity: Allows to use more than one '$\oplus$'s in any order:

$$x \oplus (y \oplus z) = (x \oplus y) \oplus z$$

Commutavity: $x \oplus y = y \oplus x$

Identity: The identity element is the n bit 0, represented by

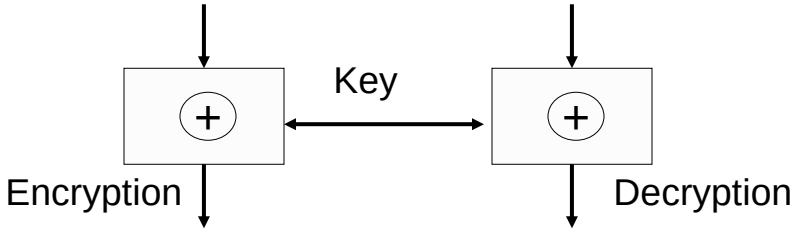
$(00...0)=0^n$

Thus, $x \oplus 0^n = x$

Inverse: Each word is the additive inverse of itself.

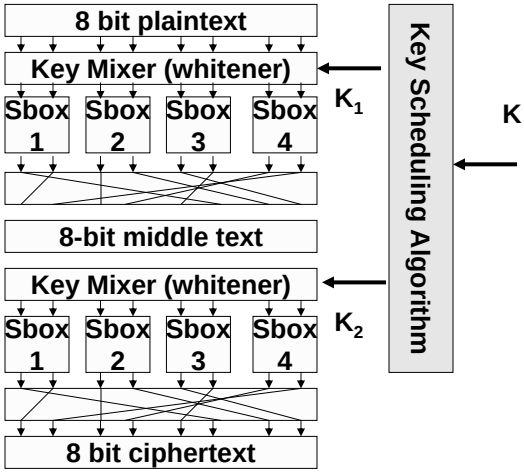
Thus, $x \oplus x = 0^n$

Application of Ex-or

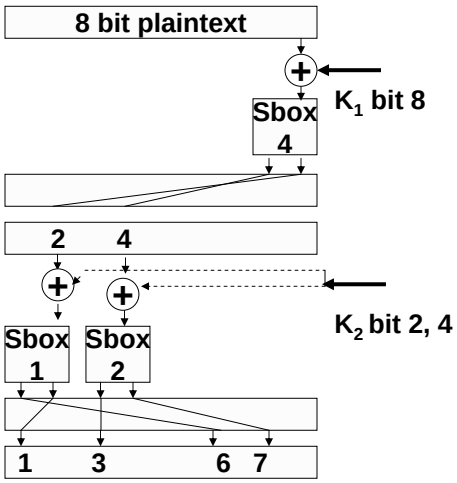


- **The key is known to both the encryptor and decryptor and helps to recover the plaintext.**

A product cipher made of 2 rounds



Diffusion and Confusion



Practical Ciphers

- Large data blocks
- More S-Boxes
- More rounds
- These help to improve the diffusion and confusion in the cipher.

Two classes of product ciphers

- Feistel Ciphers, example DES (Data Encryption Standard)
- Non-Feistel Ciphers (Substitution Permutation Networks), example AES (Advanced Encryption System)

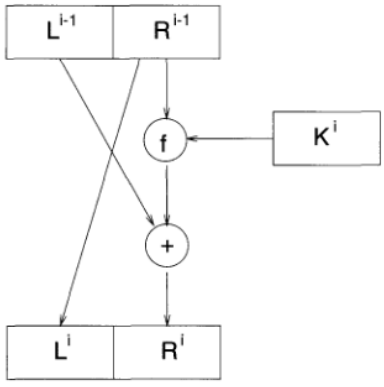
Feistel Cipher

- **Feistel cipher** refers to a type of block cipher design, not a specific cipher
- Split plaintext block into left and right halves: Plaintext = (L_0, R_0)
- For each round $i=1,2,...,n$, compute
  $\mathbf{L_i = R_{i-1}}$
  $\mathbf{R_i = L_{i-1} \oplus F(R_{i-1}, K_i)}$
  where f is **round function** and K_i is **subkey**
- Ciphertext = (L_n, R_n)

Feistel Permutation

- Decryption: Ciphertext = (L_n, R_n)
- For each round i=n,n-1,…,1, compute
  $\mathbf{R_{i-1} = L_i}$
  $\mathbf{L_{i-1} = R_i \oplus F(R_{i-1}, K_i)}$
  where f is round function and K_i is subkey
- Plaintext = (L_0, R_0)
- Formula "works" for any function F
- But only secure for certain functions F

Encryption



Repeating/ Iterating this transformation we obtain the Feistel Cipher

Non-Feistel Ciphers

- Composed of only invertible components.
- Input to round function consists of key and the output of previous round
- These functions are obtained by the repeated application of Substitution (invertible SBoxes) and Permutation.
- Thus they are called Substitution Permutation Networks (SPN).

Further Reading

- C. E. Shannon, *Communication Theory of Secrecy Systems.* Bell Systems Technical Journal, 28(1949), 656-715
- B. A Forouzan and D. Mukhopadhyay, *Cryptography & Network Security, Tata Mc Graw Hills, Chapter 5*
- Douglas Stinson, *Cryptography Theory and Practice, 2nd Edition,* Chapman & Hall/CRC