Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 17, 2015

Information Protection & Computer Security

- Lecture 1-2-3.

  Already covered topic:

  1. Security Architecture, Security Attacks, Security Services.

  2-3.Model for Network Security,Basic terms used in Cryptography, Symmetric Cipher Model, Substitution Techniques, Transpositions Techniques.

- Lecture 4.

  Today's Topic:

  Block Cipher and Stream Ciphers

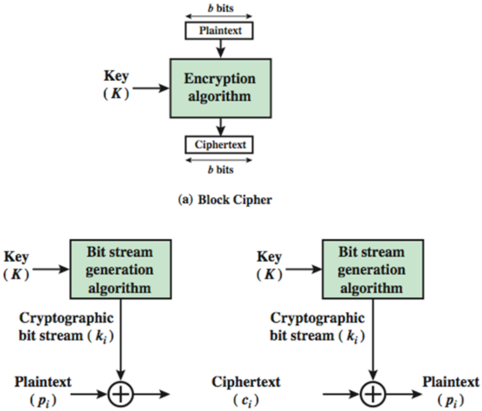
  Component of Modern Block Cipher

  Feistel Cipher Structure

  Data Encryption Standard (DES)

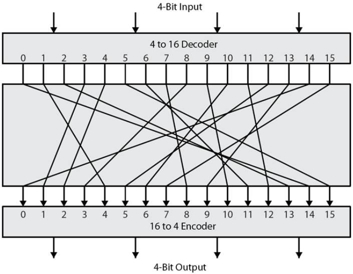
- **Block Cipher and Stream Ciphers:**

  1. Block ciphers process messages in blocks, each of which is then encrypted/decrypted like a substitution on very big characters.
  2. Stream ciphers process messages a bit or byte at a time when encrypted/decrypting.


b bits
Plaintext
Key
(K)
Encryption algorithm
Ciphertext
b bits
Key
(K)
Bit stream generation algorithm
Cryptographic bit stream (k_i)
Plaintext
(p_i)
Key
(K)
Bit stream generation algorithm
Cryptographic bit stream (k_i)
Ciphertext
(c_i)
Plaintext
(p_i)

(a) Block Cipher

- **Block Cipher Principles:**
  A block cipher operates on a plaintext block of n bits to produce a ciphertext block of n bits.
  Most symmetric block encryption algorithms are based on a structure referred to as a Feistel block cipher.
  Feistel refers to an n-bit general substitution as an ideal block cipher, because it allows for the maximum number of possible encryption mappings from the plaintext to ciphertext block.
  A 4-bit input produces one of 16 possible input states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by 4 ciphertext bits.



- **Component of Modern Block Cipher:**

  PBox (Permutation box) : It is a transposition cipher.

  SBox (Substitution box): It is a substitution cipher.

  The PBox and SBox provides:

  - Diffusion: It hides the relationships between the cipher text and the plain text.
  - Confusion: It hides the relationships between the cipher text and the key.

  The PBox is fixed and it provides Diffusion.

  The SBox is dependent on unknown key and it provides Confusion.

  Permutation:For a number 123 following are the possible permutations: 123,132,213,231,312,321........which are 3!.

- **Feistel Cipher Structure:**
  Feistel Cipher refers to a type of block cipher design.
  It splits the plaintext block into left half and right half.
  plaintext$= (L_0, R_0)$
  For each round i=1,2,3...n, compute
  $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
  where f is a round function and K_i is a subkey.
  Cipher text$= (L_n, R_n)$
- **Feistel Cipher Design Elements:** The exact realization of a Feistel network depends on the choice of the following parameters and design features:

  block size:increasing size improves security, but slows cipher.

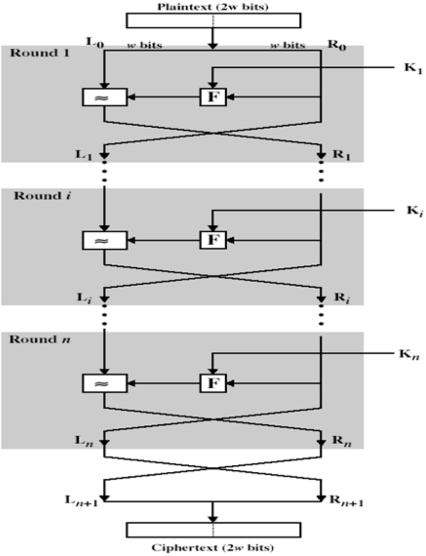
  key size:increasing size improves security, makes exhaustive key searching harder, but may slow cipher.

  number of rounds:increasing number improves security, but slows cipher.

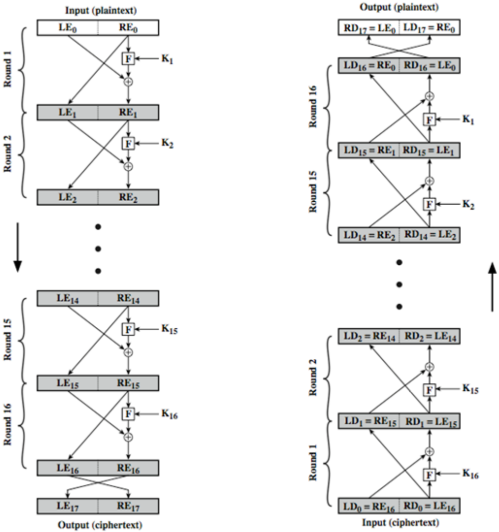
  subkey generation algorithm:greater complexity can make analysis harder, but slows cipher.

  round function:greater complexity can make analysis harder, but slows cipher.

Classical Feistel Network



- **Feistel Cipher Structure:**



- **Data Encryption Standard (DES):**
- IBM developed Lucifer cipher:
  - by team led by Horst Feistel.
  - used 64-bit data blocks with 128-bit key.
  - then redeveloped as a commercial cipher.
  - in 1973 NBS (National Bureau of Standards) issued request for proposals for a national cipher standard.
  - IBM submitted their revised Lucifer which was eventually accepted as the DES.
- In DES, plaintext must be 64 bits in length and key is 56 bits in length.
- The basic process in enciphering a 64-bit data block using the DES, consists of:

  - an initial permutation (IP)

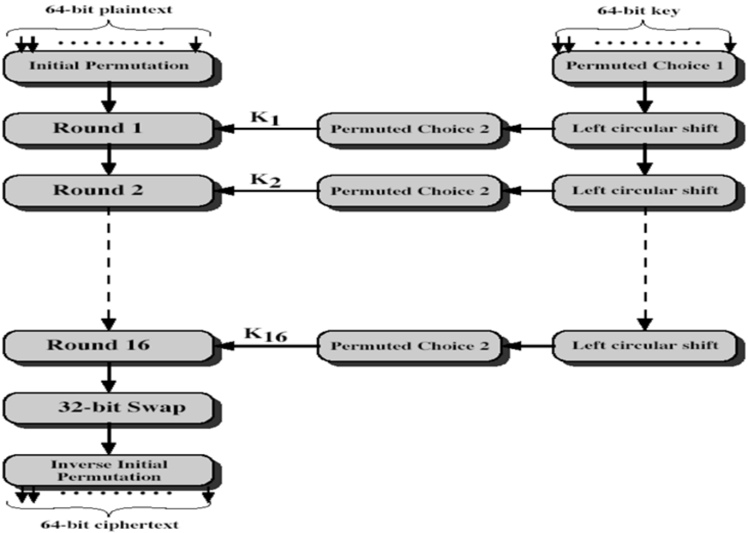
  - 16 rounds of a complex key dependent round function involving substitution and permutation functions

  - a final permutation, being the inverse of IP
- The right side (Diagram on next slide) shows the handling of the 56-bit key and consists of:

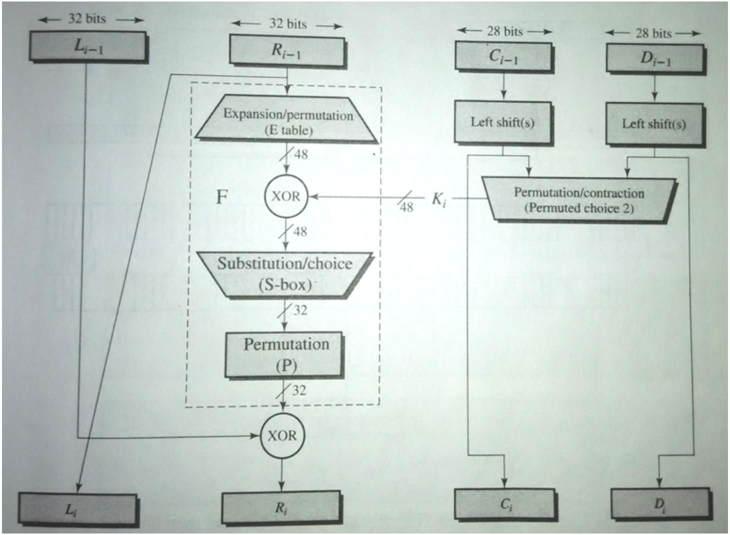
  - an initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves

  - 16 stages to generate the subkeys using a left circular shift and a permutation

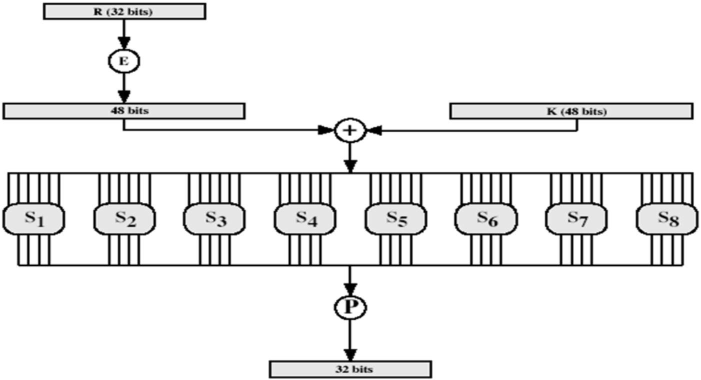
Data Encryption Standard (DES):



- **Data Encryption Standard (DES):**Single Round of DES:

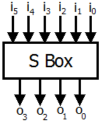


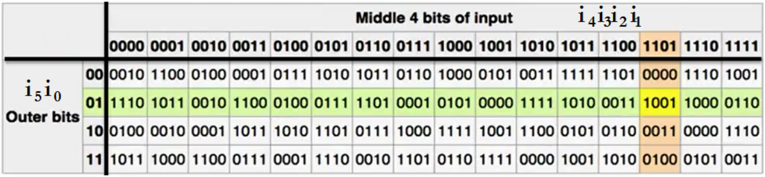
- **Data Encryption Standard (DES):** Substitution Box(S-Box):



- **Data Encryption Standard (DES):**

S-Box table lookup





		Middle 4 bits of input $i_4i_3i_2i_1$															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
i_5i_0 **Outer bits**	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Expansion/permutation (E table)
input word: ....efgh ijkl mnop...........
output word: ..... defghi hijklm lmnopq...........