Feistal Ciphers Structure

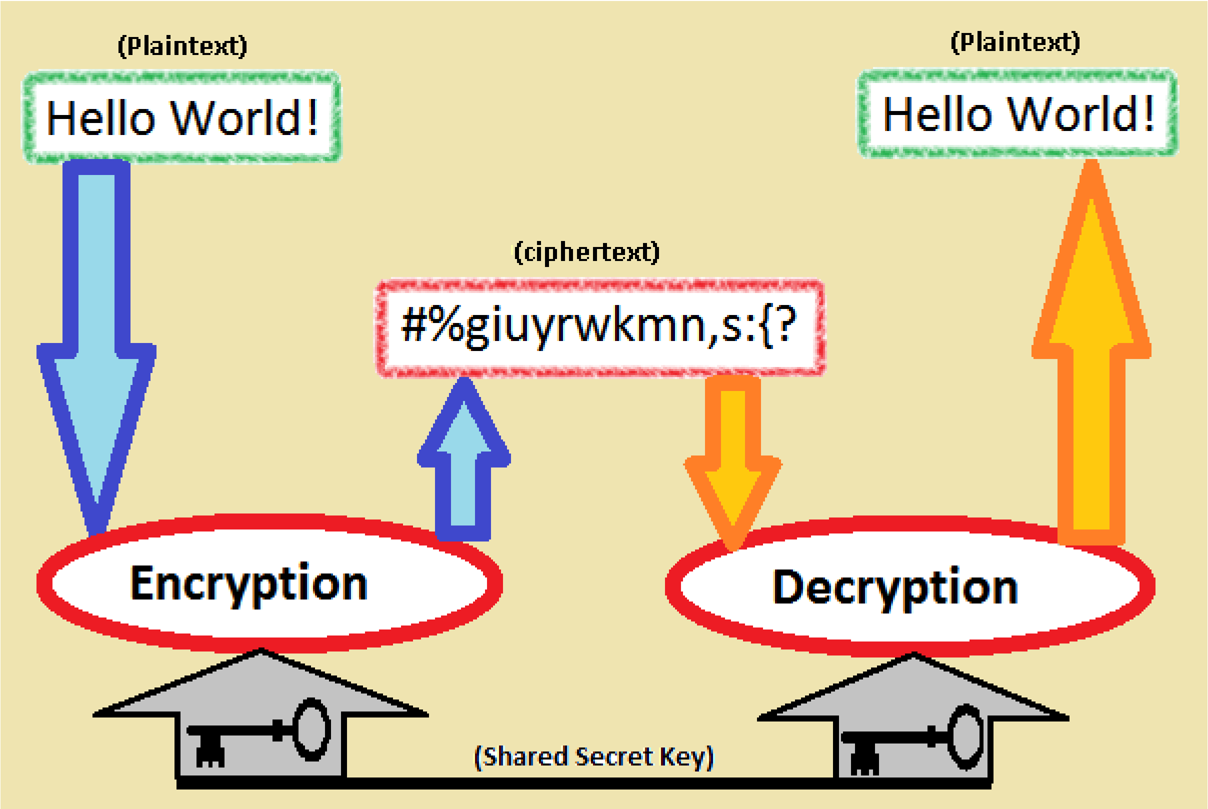
Dr Priya Matta

Overview

- Cipher
- Block Ciphers
- Block vs. Stream Ciphers
- Block Cipher Principles
- Substitution-Permutation Ciphers
- Diffusion and Confusion
- Feistel Cipher Structure
- Feistel Cipher Design Principles

Cipher

- In cryptography , a cipher (or cypher) is an algorithm for performing encryption or decryption.
  - a series of well-defined steps that can be followed as a procedure.
- Cryptography (or cryptology; from Greek is the practice and study of hiding information.


(Plaintext)
Hello World!
(Plaintext)
Hello World!
(ciphertext)
#%giuyrwkmn,s:{?
Encryption
Decryption
(Shared Secret Key)

Block Ciphers

One of the most widely used types of cryptography algorithms.

- Provide strong secrecy and/or authentication services
- In particular will introduce DES (Data Encryption Standard)

Block vs Stream Ciphers

Block ciphers process messages into blocks, each of which is then en/decrypted

- like a substitution on very big characters
  - 64-bits or more

Stream ciphers process messages a bit or byte at a time when en/decrypting

- many current ciphers are block ciphers
- hence are focus of course

Block Cipher Principles

- block ciphers look like an extremely large substitution
- would need table of 2^{64} entries for a 64-bit block
  - 64-bit general substitution block cipher, key size 2^{64}!
- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- needed since must be able to **decrypt** ciphertext to recover messages efficiently

Substitution-Permutation Ciphers

- in 1949 Shannon introduced idea of substitution-permutation (S-P) networks
  - modern substitution-transposition product cipher
- these form the basis of modern block ciphers
- S-P networks are based on the two primitive cryptographic operations we have seen before:
  - substitution (S-box)
  - permutation (P-box) (transposition)
- provide confusion and diffusion of message

Diffusion and Confusion

- Introduced by Claude Shannon to thwart cryptanalysis based on statistical analysis
  - Assume the attacker has some knowledge of the statistical characteristics of the plaintext
- cipher needs to completely obscure statistical properties of original message
- a one-time pad does this

Diffusion and Confusion

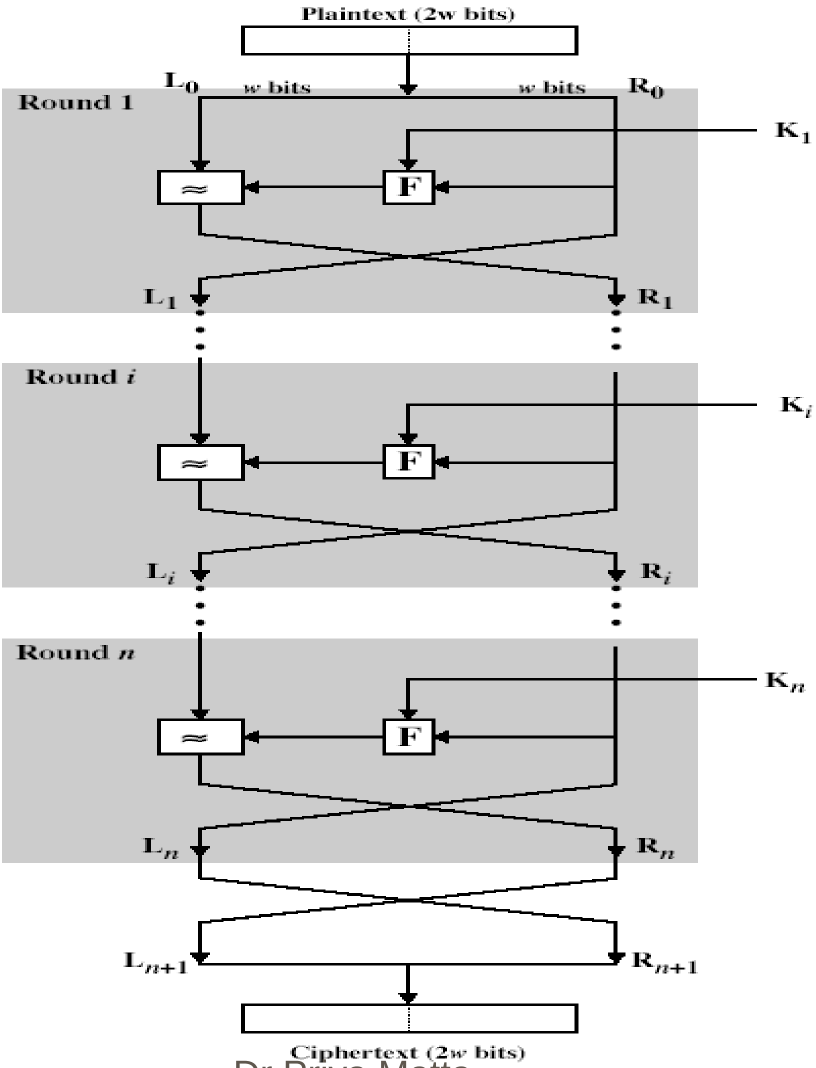
More practically Shannon suggested combining elements to obtain:

- **Diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- **Confusion** – makes relationship between ciphertext and key as complex as possible

Feistel Cipher Structure

- Horst Feistel devised the **feistel cipher**
  - implements Shannon’s substitution-permutation network concept
- partitions input block into two halves
  - process through multiple rounds which
  - perform a substitution on left data half
  - based on round function of right half & subkey
  - then have permutation swapping halves

Feistel Cipher Structure



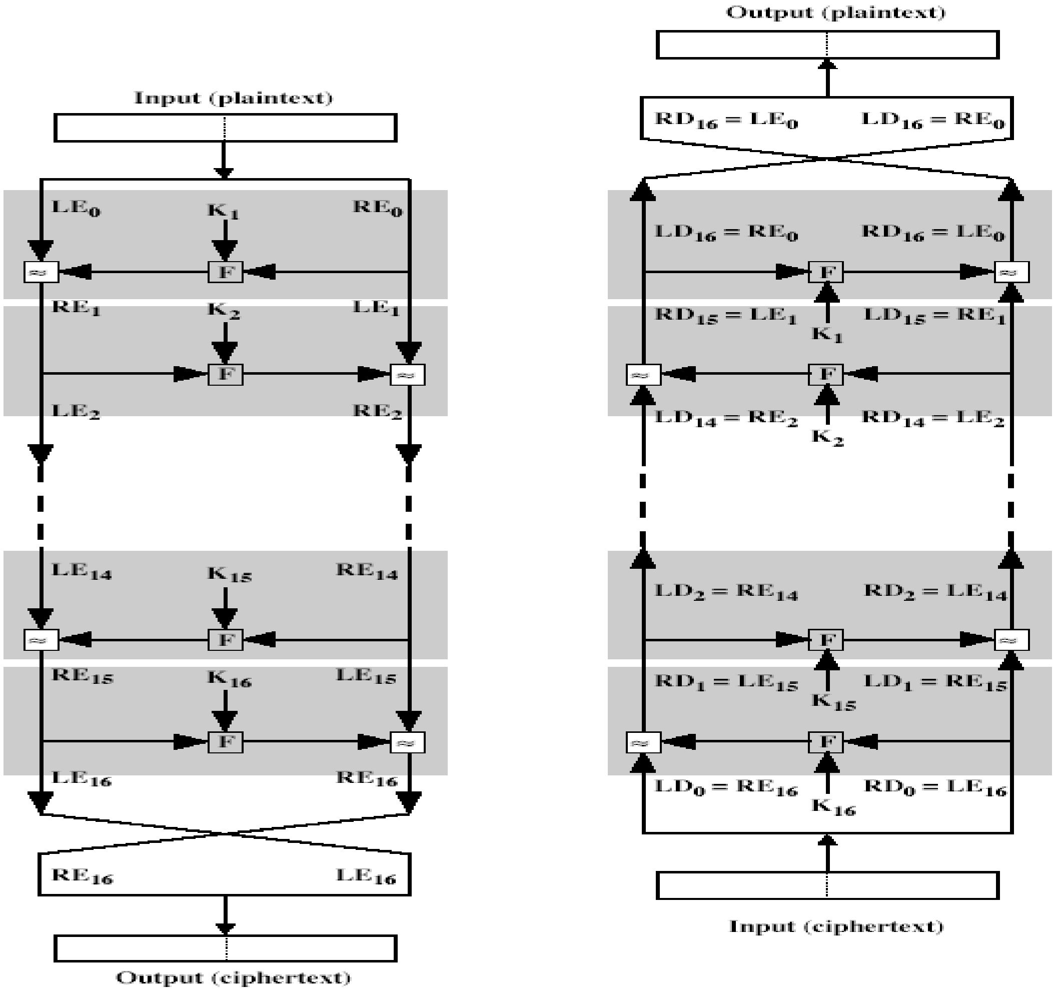
Feistel Cipher

- n sequential rounds
- A substitution on the left half L_i
  - 1. Apply a round function F to the right half R_i and
  - 2. Take XOR of the output of (1) and L_i
- The round function is parameterized by the subkey K_i
  - K_i are derived from the overall key K

Feistel Cipher Design Principles

- **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**
  - greater complexity can make analysis harder, but slows cipher
- **round function**
  - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption & ease of analysis**
  - are more recent concerns for practical use and testing

Feistel Cipher Decryption


Input (plaintext)
LE_0
K_1
RE_0
F
RE_1
K_2
LE_1
F
LE_2
RE_2
LE_{14}
K_{15}
RE_{14}
F
RE_{15}
K_{16}
LE_{15}
F
LE_{16}
RE_{16}
RE_{16}
LE_{16}
Output (ciphertext)
Output (plaintext)
$RD_{16} = LE_0$
$LD_{16} = RE_0$
$LD_{16} = RE_0$
$RD_{16} = LE_0$
F
$RD_{15} = LE_1$
$LD_{15} = RE_1$
K_1
F
$LD_{14} = RE_2$
$RD_{14} = LE_2$
K_2
$LD_2 = RE_{14}$
$RD_2 = LE_{14}$
F
$RD_1 = LE_{15}$
$LD_1 = RE_{15}$
K_{15}
F
$LD_0 = RE_{16}$
$RD_0 = LE_{16}$
K_{16}
Input (ciphertext)