PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

Private key Systems

Lecture 3

Feistel Cipher

Used by DES

Types of Symmetric key cipher

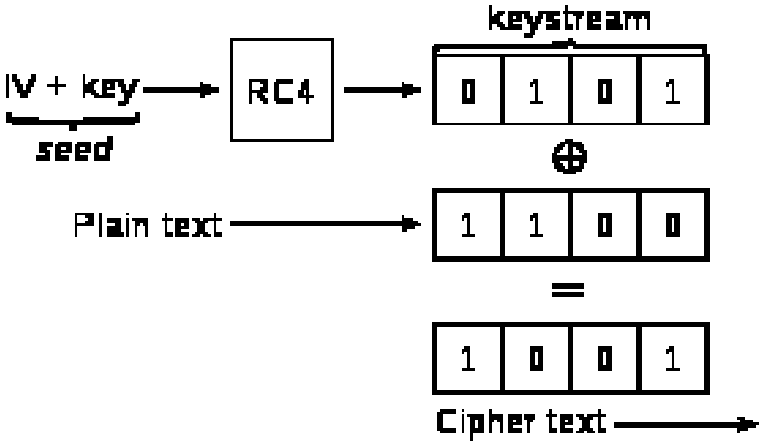
- ***Stream cipher:***
  - algorithm operates on individual bits (or bytes) one at a time
  - Example RC4 cipher system
- ***Block cipher:***
  - operates on fixed-length groups of bits called blocks
  - Example DES, Triple DES and AES

Stream Cipher (Rivest Cipher 4)

- Key stream
  - Pseudo-random sequence of bits S = S[0], S[1], S[2], …
  - Can be generated on-line one bit (or byte) at the time
- Stream cipher
  - XOR the plaintext with the key stream C[i] = S[i] ⊕ P[i]
  - Suitable for plaintext of arbitrary length generated on the fly, e.g., media stream

RC4

- **Wired Equivalent Privacy** (WEP deprecated in 2004) used the stream cipher RC4 for confidentiality.



Limitations of stream cipher

- Keystream must have a large ***period*** and it must be impossible to ***recover the cipher's key*** or internal state from the keystream.
- One never reuse the same keystream twice
    - different ***nonce or key*** must be supplied

Block cipher

- Partition the text into relatively large (e.g. 128 bits) blocks and encode each block separately.
- The encoding of each block generally depends on at most one of the previous blocks.
- The same “key” is used at each block.

Difference between block and stream ciphers

- Block ciphers work a on block / word at a time, which is some number of bits. All of these bits have to be available before the block can be processed.
- Block cipher uses either 64 bits or more than 64 bits.
- The complexity of block cipher is simple.

- Stream ciphers work on a bit or byte of the message at a time, hence process it as a “stream”.
- While stream cipher uses 8 bits.
- While stream cipher is more complex.

Difference between block and stream ciphers

- Block cipher Uses confusion as well as diffusion.
- In block cipher, reverse encrypted text is hard.
- The algorithm modes which are used in block cipher are: ECB (Electronic Code Book) and CBC (Cipher Block Chaining).

- While stream cipher uses only confusion.
- While in stream cipher, reverse encrypted text is easy.
- The algorithm modes which are used in stream cipher are: CFB (Cipher Feedback) and OFB (Output Feedback).

Confusion and diffusion

- Diffusion:
  - Refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.
  - Makes statistical relationship between the plaintext and ciphertext as complex as possible

- Confusion:
  - Refers to making the relationship between the ciphertext and the symmetric key as complex and involved as possible;
  - Makes relationship between ciphertext and key as complex as possible

Block cipher design principle

- ***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

Feistel cipher

- Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived.
- DES is just one example of a Feistel Cipher.
- DES is a cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption

History

- Feistel Cipher: the fundamental building block of DES designed by IBM.
- DES was adopted as a US federal standard for commercial encryption in 1975.
- Design requirements:
  - must provide high level of security (commercial standard)
  - Security must not depend on secrecy of algorithm (Kerckhoff’s principle)
  - Must be easily and economically implemented

Feistel cipher structure

- Horst Feistel derived the Feistel cipher based on invertible product cipher
- process
  - 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 and subkey permutation
  - swapping both left and right partition
- Implements Shannon's SP net concept

Feistel Cipher: a cipher design pattern

- Encryption :N rounds
- Plaintext = (L0, R0)

  1 <= i <= n

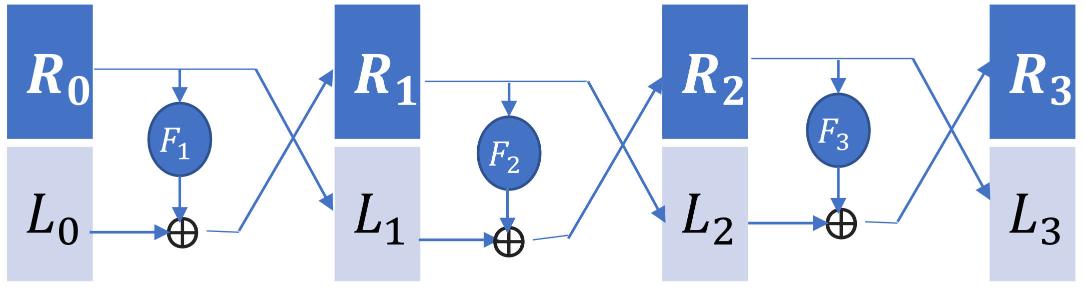
  Li = Ri-1

  Ri = Li-1 xor f(Ri-1 , Ki)

  Subkeys Ki derived from key K

  Ciphertext = (Rn, Ln) Note: swapped halves
- Decryption: As Encryption above, but subkeys applied in reverse order: N, N-1, N-2, …

Feistel Cipher for 3 rounds



input

Output

F: $K^3\ X\ \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}\ is\ a\ secure\ PRP$

Page 212 FIGURE 6.5: A three-round Feistel network.

Thank you

Next Class

- ☞ Mandatory reading for the next class
  - ☞ https://www.oreilly.com/library/view/computer-security-and/9780471947837/sec9.3.html

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT

PESU Center for Internet of Things