Computer Security

Block ciphers

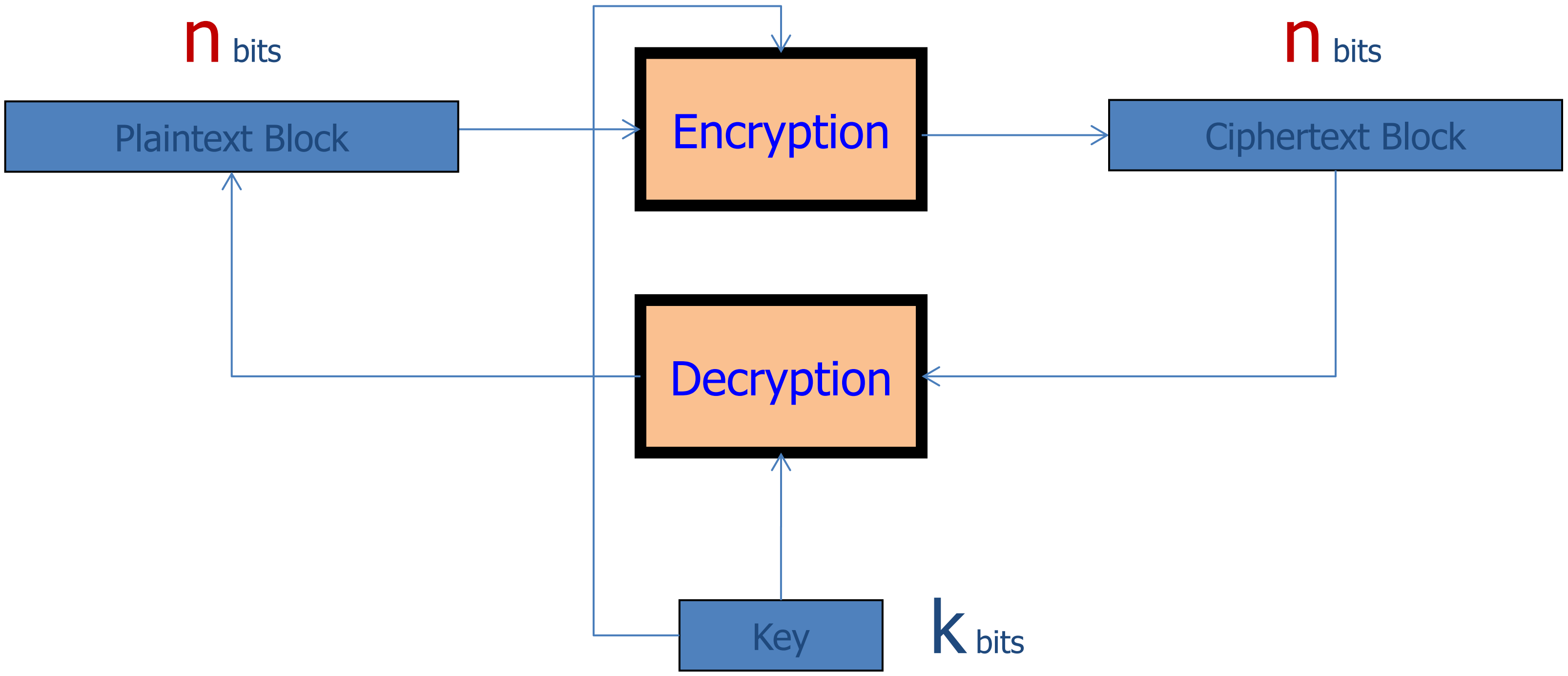
Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Block ciphers - basic structure

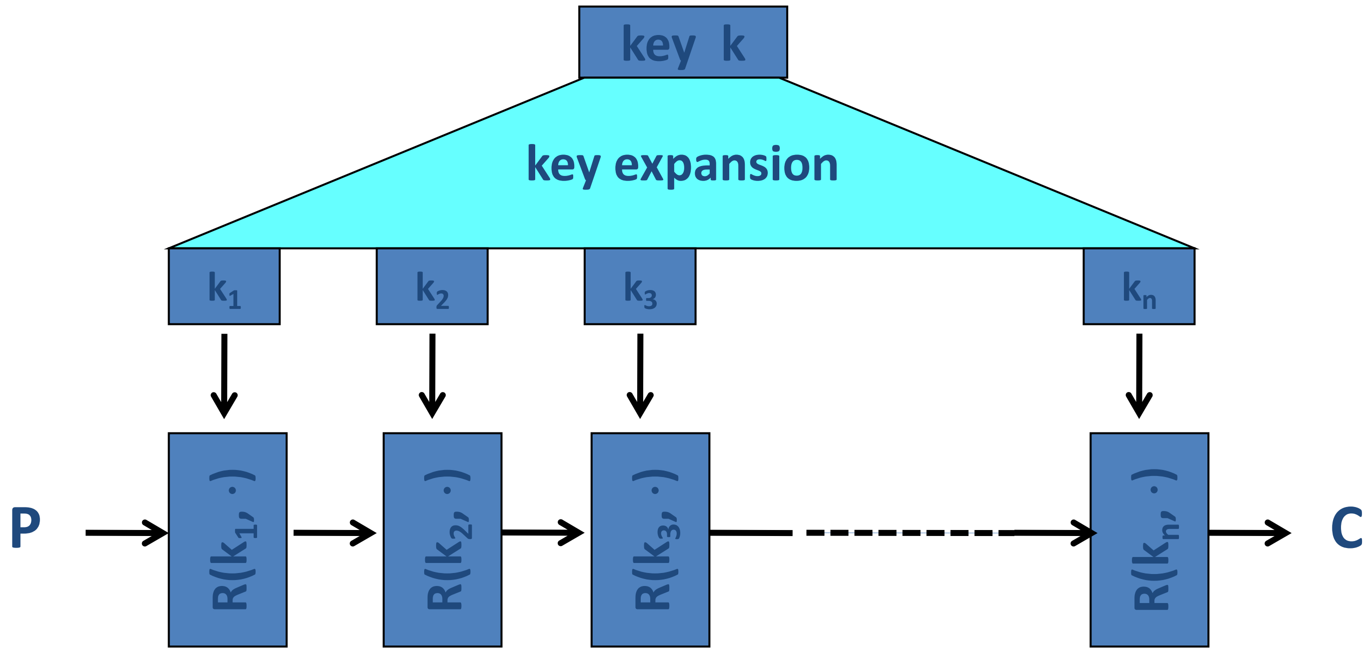


Canonical examples:

1. DES: n= 64 bits, k = 56 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

Block ciphers built by iteration

Iterate substitution and permutation (by Shannon, 1948)



R(k,m) is called a round function

for DES (n=16), for AES-128 (n=10)

Cipher structures

- Feistel structure
  - This technique was devised by Horst Feistel of IBM 
  - Each round uses an operation called the F-function whose input is half a block and a round key; the output is a half-block of scrambled data which is XOR-ed into the other half-block of text
  - Examples: DES
- Substitution-Permutation (SP) networks
  - Shannon's own design for a product cipher
  - 2 layers in each round: a substitution layer provides confusion, then a permutation layer provides diffusion
  - Examples: AES

To be secure, every cipher must contain ***nonlinear*** operations.

Feistel Cipher: Encryption

- **Feistel cipher** is a type of block cipher, not a specific block cipher
- Split plaintext block into left and right halves: $P = (L_0, R_0)$
- For each round $i = 1, 2, \ldots, n$, compute

  $L_i = R_{i-1}$

  $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

  where F is **round function** and K_i is **subkey**
- Ciphertext: $C = (L_n, R_n)$

Feistel Cipher: Decryption

- Start with ciphertext $C = (L_n, R_n)$
- For each round $i = n, n-1, \ldots, 1$, compute

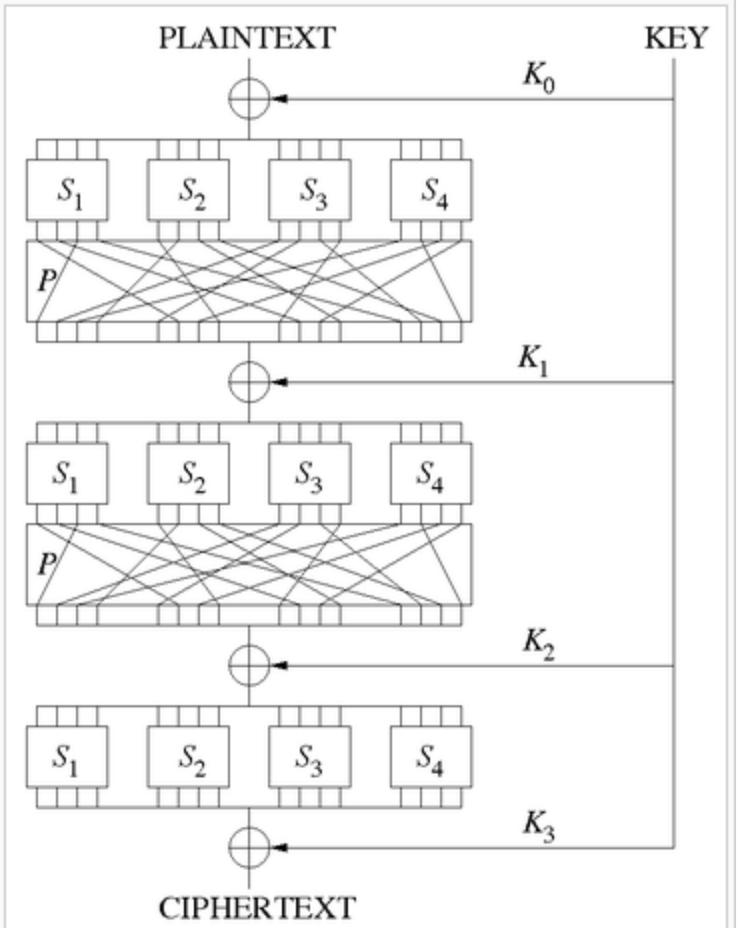
  $R_{i-1} = L_i$

  $L_{i-1} = R_i \oplus F(R_{i-1}, K_i)$

  where F is round function and K_i is subkey
- Plaintext: $P = (L_0, R_0)$
- Formula "works" for any function F
  - But only secure for certain functions F

SP networks

- More constraints on the round function: must be invertible
- Faster than Feistel-structure
- Parallel computation
- Typically E ≠ D



A sketch of a Substitution-Permutation Network with 3 rounds,

Quiz

Q1. What is the main advantage of a Feistel cipher over an SP network?

The F-function itself need not be reversible. This gives the designer extra flexibility; almost any operation he can think up can be used in the F-function

Q2. What is the main advantage of an SP network over a Feistel cipher?

In the Feistel construction, only half the output changes in each round while an SP network changes all of it in a single round

Questions?


Sungkyunkwan
Campus
campus
established
Sciences
University
university
Suwon
School
Graduate
Seoul
Natural
Korean
edit
constructed
English
Social
Global
Building
Institute
Professors
Confucian
Humanities
lecturers
schools
Science
Advanced
Education
Engineering
located
Joseon
Korea
Zone
Academic
ASLE-Korea
Administration
Hall
also
two
four
city
now
one