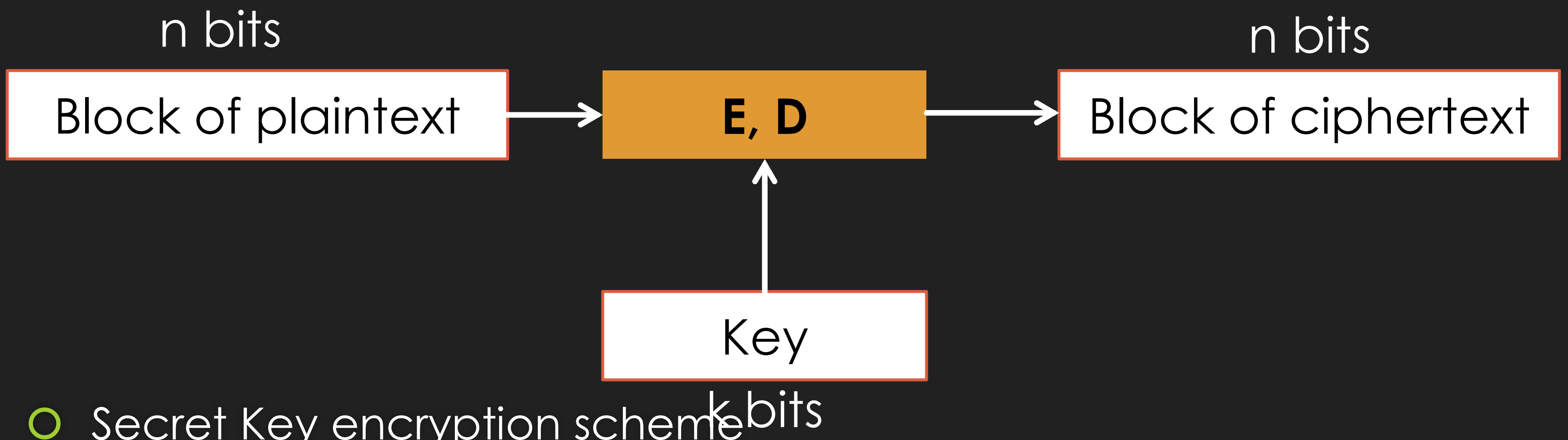
An Introduction to Block Ciphers

Overview

- 원래 메시지 = Plaintext block input; 암호문 = ciphertext block output
- Block ciphers made via iteration
- 유명한 block ciphers: triple DES, AES
- Pseudo Random Functions and Pseudo Random Permutations
- Secure block ciphers

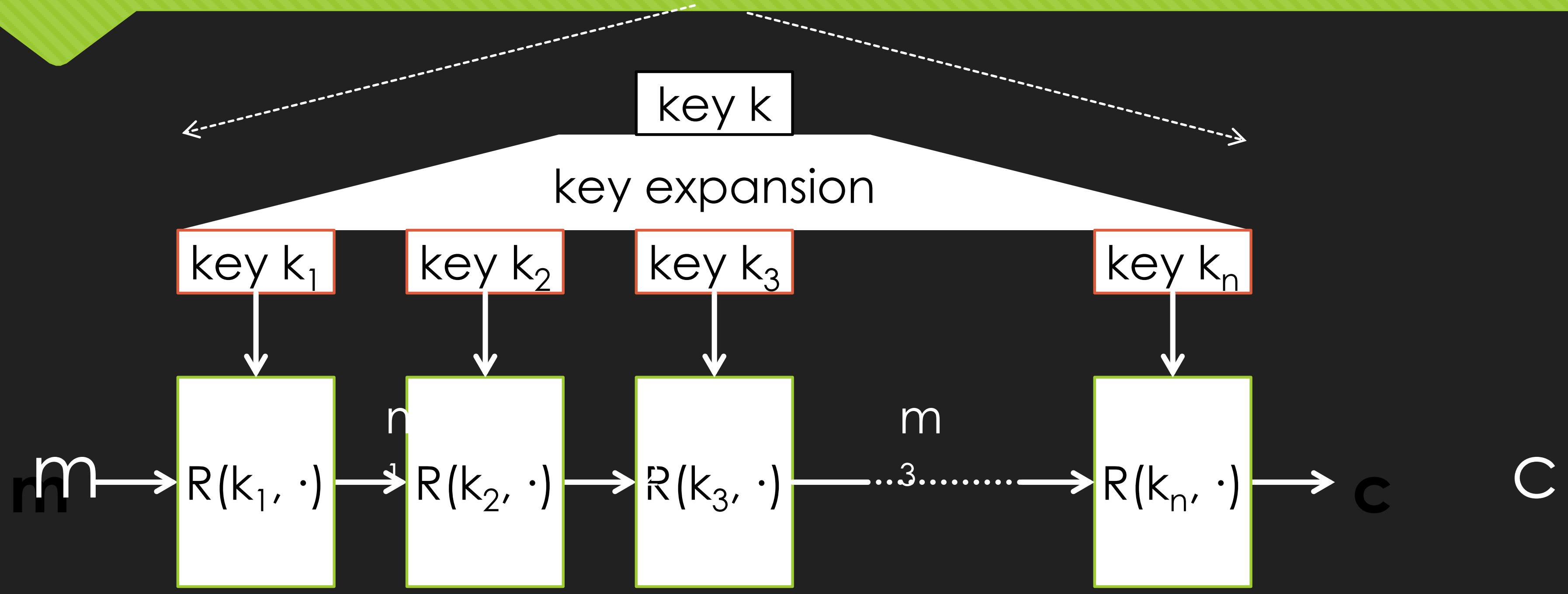
What is a block cipher?

- Used to translate the plaintext to ciphertext in blocks and vice versa
- Plaintext block of certain size N bits → ciphertext block of same size



- Secret Key encryption scheme

How are block ciphers made?



R(k, m) is called a *round function*

Ex: 3DES (n=48), AES128 (n=10)

3DES vs AES

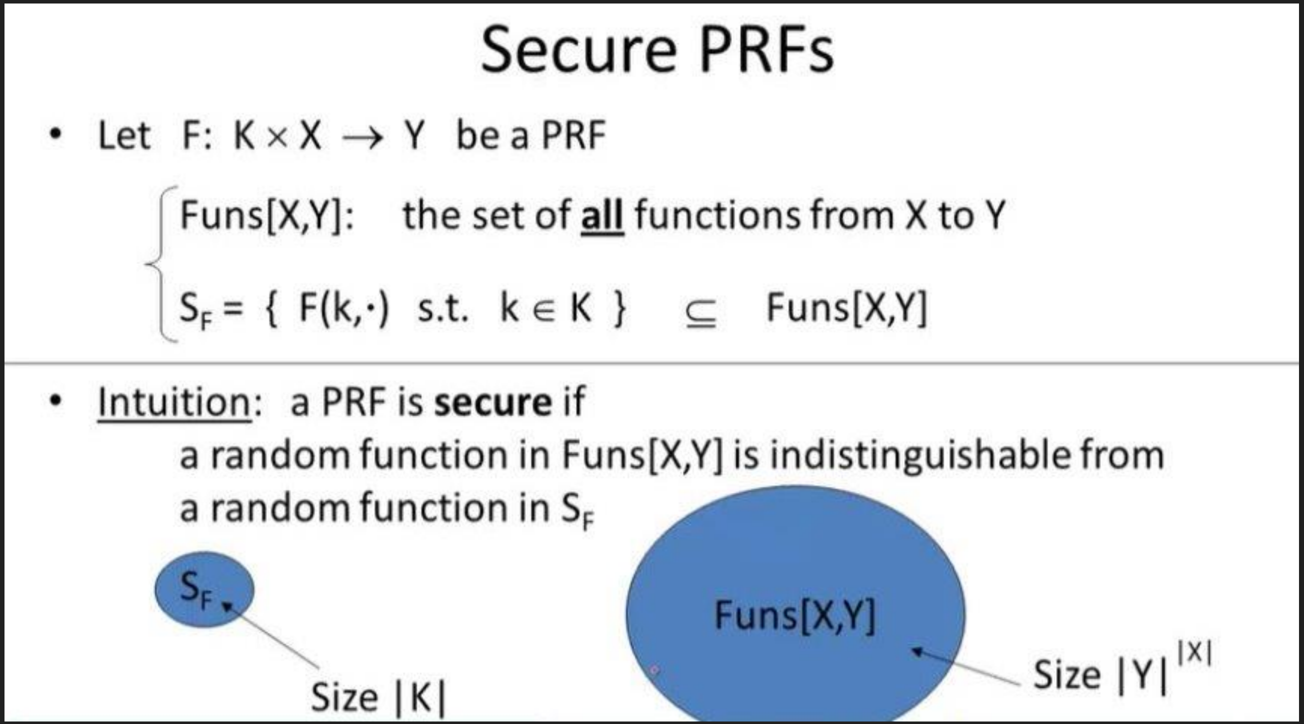
- 3DES: block size = 64 bit; total types of blocks = 2^64; key size = 168 bit; speed = 13 MB/sec
- AES-128: block size = 128 bit; total types of blocks = 2^128; key size = 128 bit; speed = 109 MB/sec
- 3DES has 48 rounds; AES-128 has 10 rounds

What are PRPs and PRFs?

- K = key
- X = set of all input bits in input block
- Y = set of all output bits in output block; note Y does not necessarily = X.
- **Pseudo random permutations (PRPs):** similar to block ciphers; take inputs K,X and output X
- **Pseudo random functions (PRFs):** take inputs K, X and output Y

Secure block ciphers

- Secure block ciphers = Good PRP



Secure PRFs

- Let F: $K \times X \rightarrow Y$ be a PRF

$$\begin{cases} \text{Funs[X,Y]: the set of } \underline{\textbf{all}} \text{ functions from X to Y} \\ S_F = \{\ F(k,\cdot)\ \text{ s.t. } k \in K\ \} \subseteq \text{Funs[X,Y]} \end{cases}$$

- Intuition: a PRF is **secure** if

  a random function in Funs[X,Y] is indistinguishable from a random function in S_F

S_F
Size |K|
Funs[X,Y]
Size $|Y|^{|X|}$