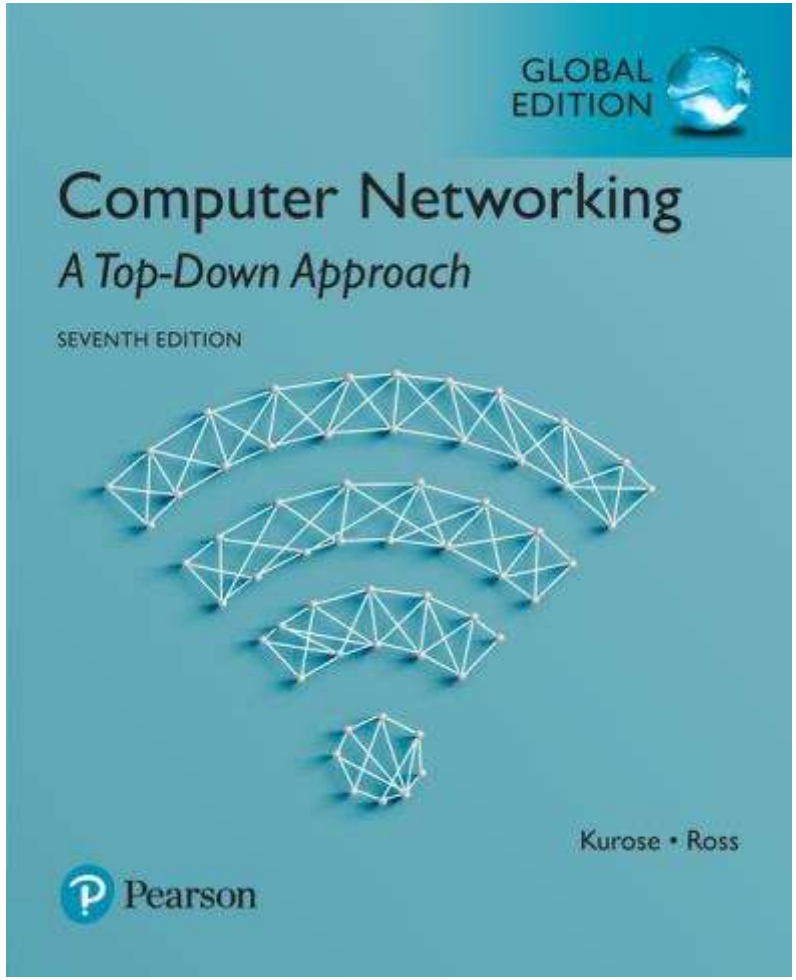
제27강
네트워크 보안과 대칭키 암호

Computer Networking: A Top Down Approach

컴퓨터 네트워크
(2019년 1학기)

박승철교수

한국기술교육대학교
컴퓨터공학부



Pre-study Test :

1) 다음 중 메시지의 기밀성(confidentiality)를 유지하기 위한 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 디지털 서명(digital signature)
④ 메시지 해싱(hashing)

2) 다음 중 송신자의 신원(identity)을 확인하는 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 메시지 해싱(hashing)
④ 방화벽(firewall)

3) 다음 중 메시지 무결성(integrity)을 확인하는 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 메시지 해싱(hashing)
④ 방화벽(firewall)

4) 다음 중 시스템의 가용성(availability)를 훼손하는 공격은?

① 도청(eavesdrop)
② 가장(impersonation)
③ 하이재킹(hijacking)
④ DoS(Denial of Service)

5) 다음 중 암호화 기술에 대한 설명 중 틀린 것은?

① 대칭키 암화화(symmetric key encryption)은 1개의 키를 사용한다.
② 공개키 암호화(public key encryption)은 2개의 키를 사용한다.
③ 공개키 암호화(public key encryption)은 2개의 키를 모두 공개한다.
④ 공개키 암호화는 암호화와 복호화에서 서로 다른 키를 사용한다.

6) 다음 중 대칭키 암호화 기술이 아닌 것은?

① DES
② 3DES
③ RSA
④ AES

7) 암호에 사용된 키를 알아내기 위해 모든 경우의 수를 시도하는 공격을 무엇이라 하는가?

① 추측 공격(guessing attack)
② 사전 공격(dictionary attack)
③ 도청 공격(eavesdrop attack)
④ 전사 공격(brute force attack)

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity, authentication

8.4 Securing e-mail

8.5 Securing TCP connections: SSL

8.6 Network layer security: IPsec

8.7 Securing wireless LANs

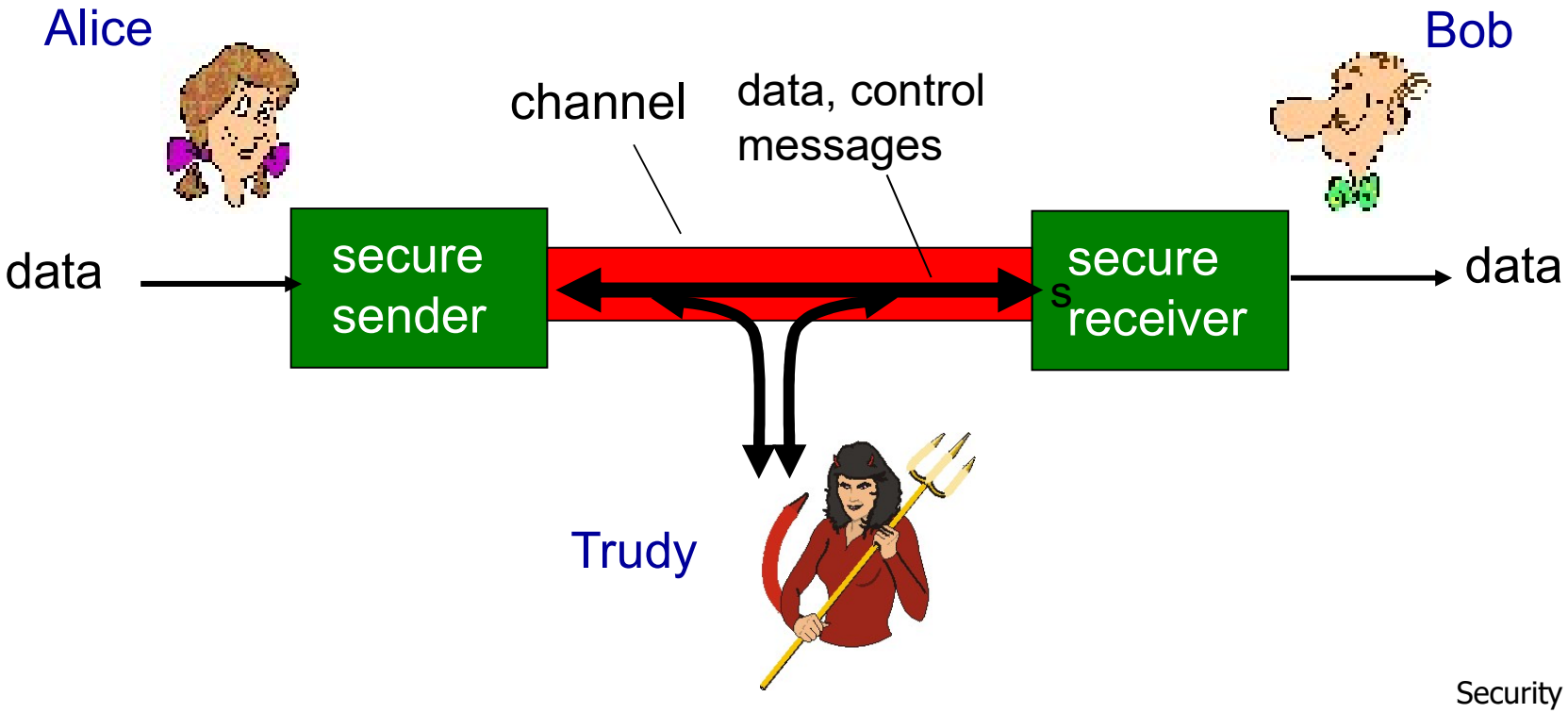
8.8 Operational security: firewalls and IDS

What is network security?

1. *Confidentiality(기밀성)*: only sender, intended receiver should "understand" message contents
   - sender encrypts message
   - receiver decrypts message
2. *Authentication(인증)*: sender, receiver want to confirm identity of each other
3. *message integrity(메시지 무결성)*: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
4. *access and availability(접근 및 가용성)*: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: A lot! See section 1.6

- *Eavesdrop(도청):* intercept messages
- actively *insert* messages into connection(메시지 삽입/조작)
- *Impersonation(가장):* can fake (spoof) source address in packet (or any field in packet)
- *Hijacking(연결 하이재킹):* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service(서비스 거부):* prevent service from being used by others (e.g., by overloading resources)

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message integrity, authentication

8.4 Securing e-mail

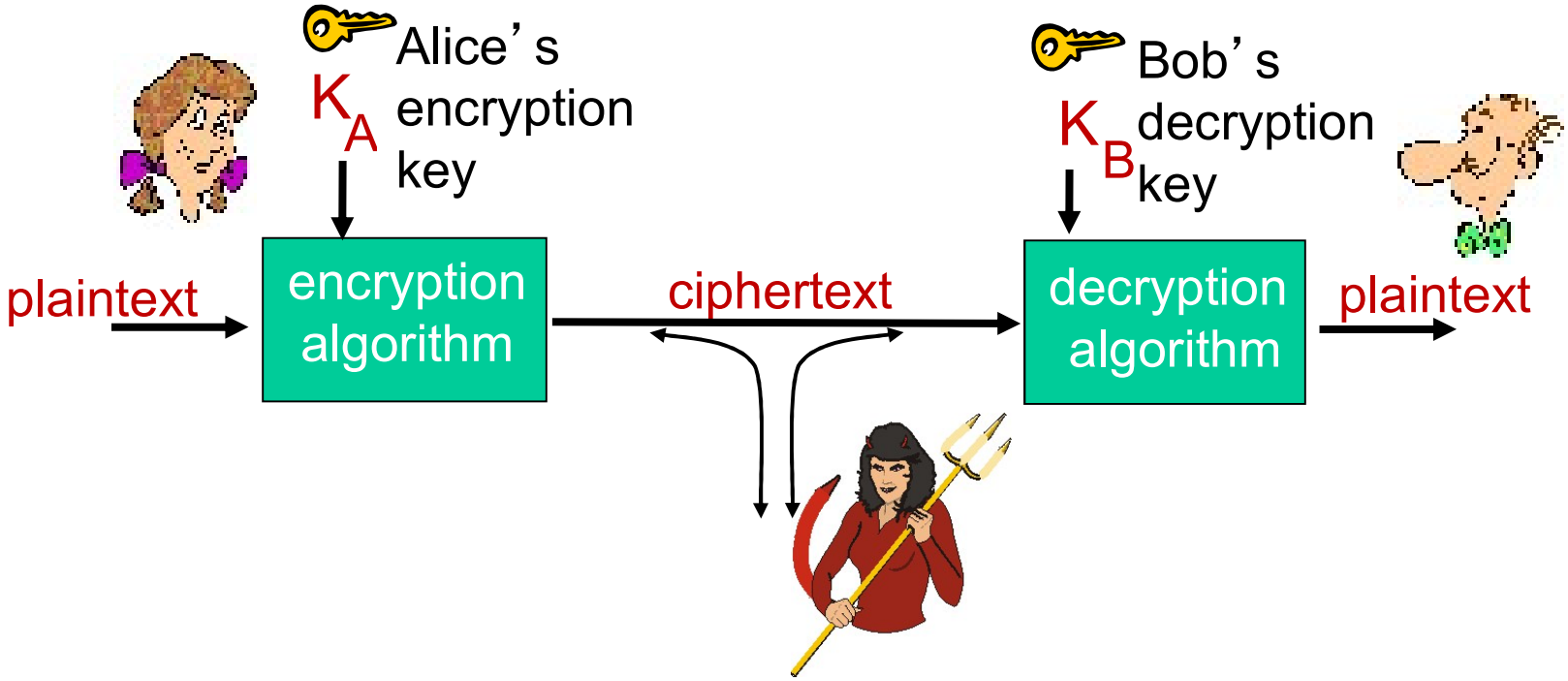
8.5 Securing TCP connections: SSL

8.6 Network layer security: IPsec

8.7 Securing wireless LANs

8.8 Operational security: firewalls and IDS

The language of cryptography

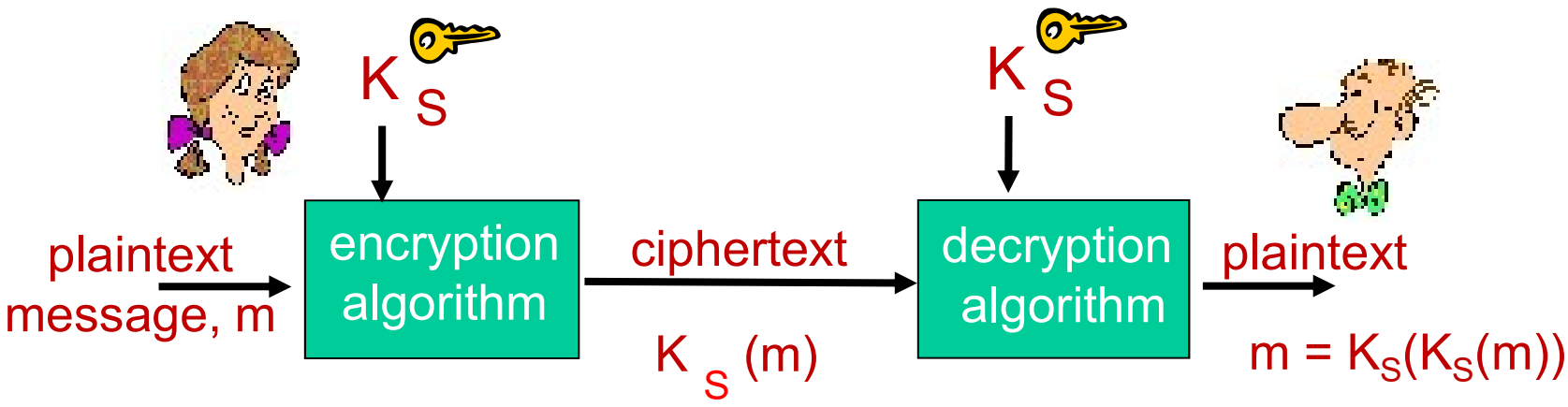


m plaintext message(평문)

$K_A(m)$ ciphertext(암호문), encrypted with key K_A

$m = K_B(K_A(m))$

Symmetric key(대칭키) cryptography

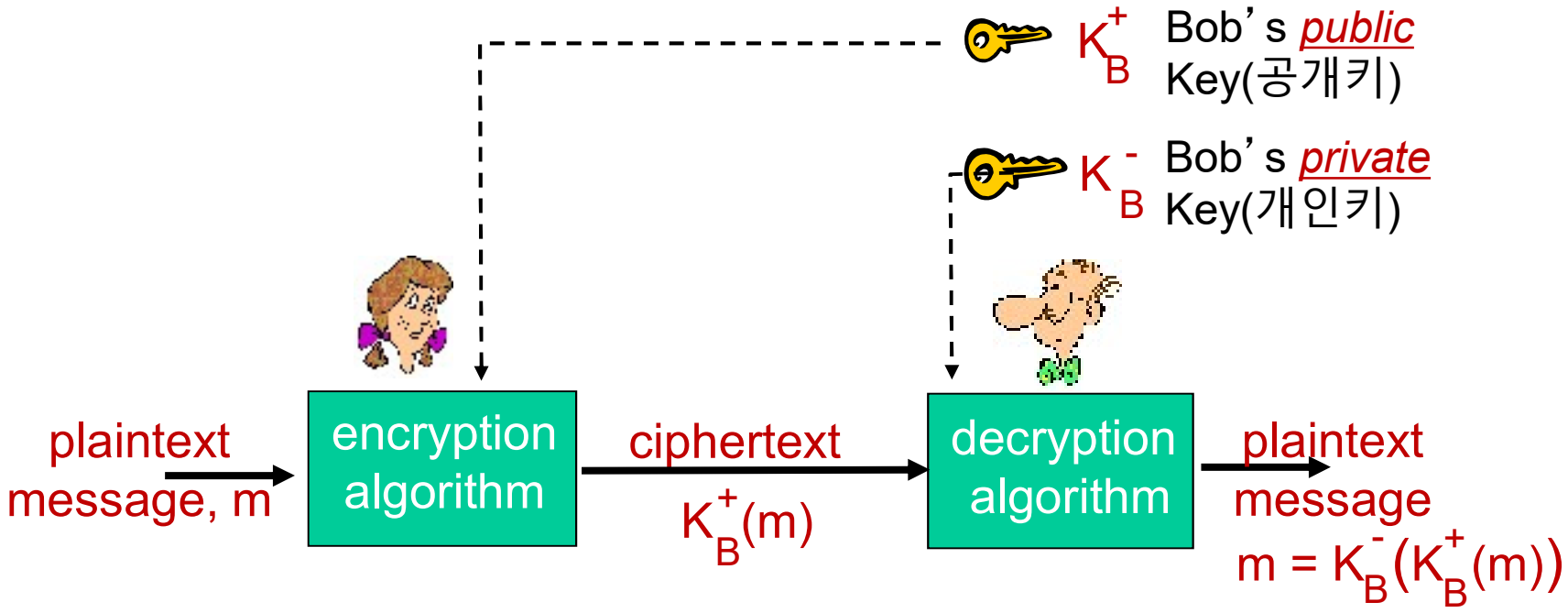


symmetric key crypto: Bob and Alice share same (symmetric) key: K_S

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Q: how do Bob and Alice agree on key value?

Public key cryptography



Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- block cipher with cipher block chaining
- how secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase decrypted (brute force) in less than a day
  - no known good analytic attack
- making DES more secure:
  - 3DES: encrypt 3 times with 3 different keys

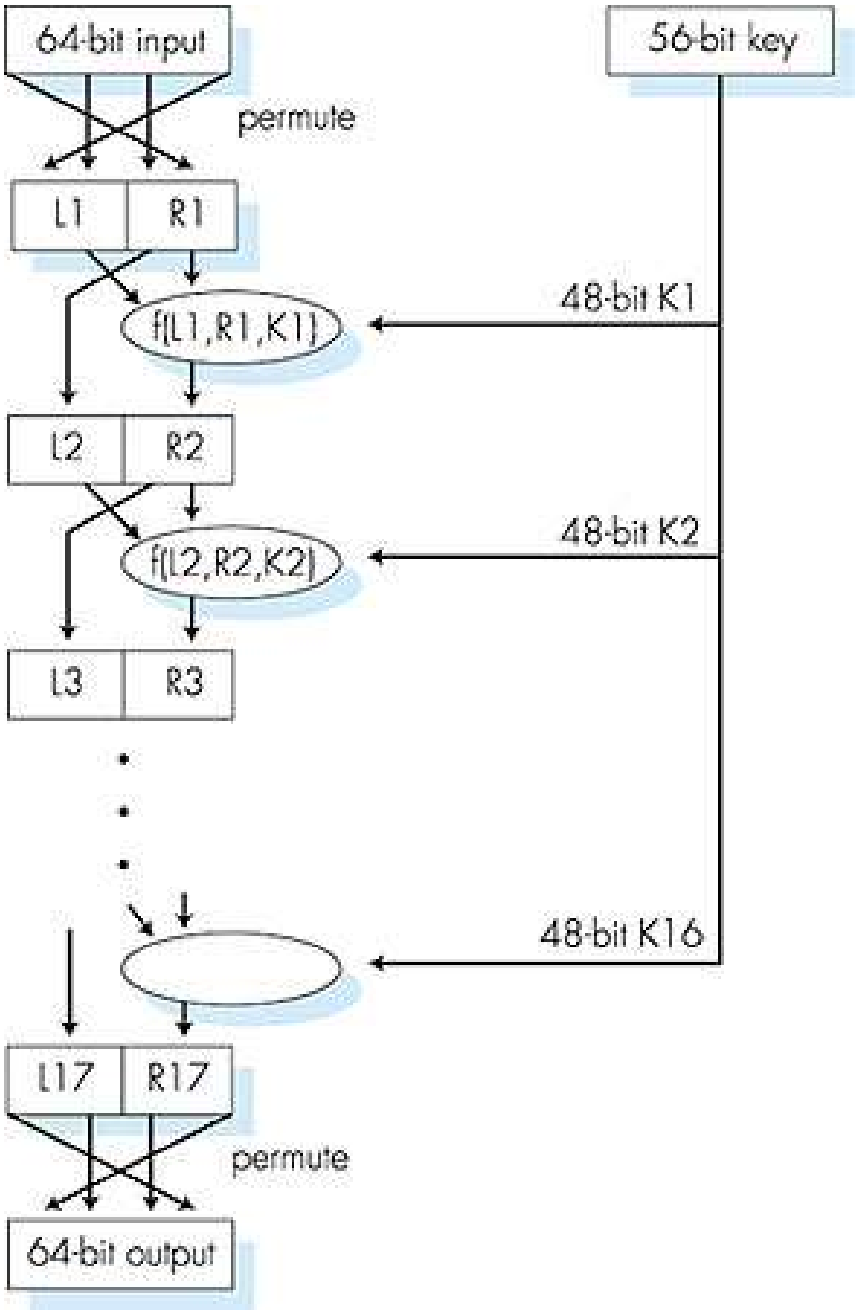
Symmetric key crypto: DES

DES operation

initial permutation

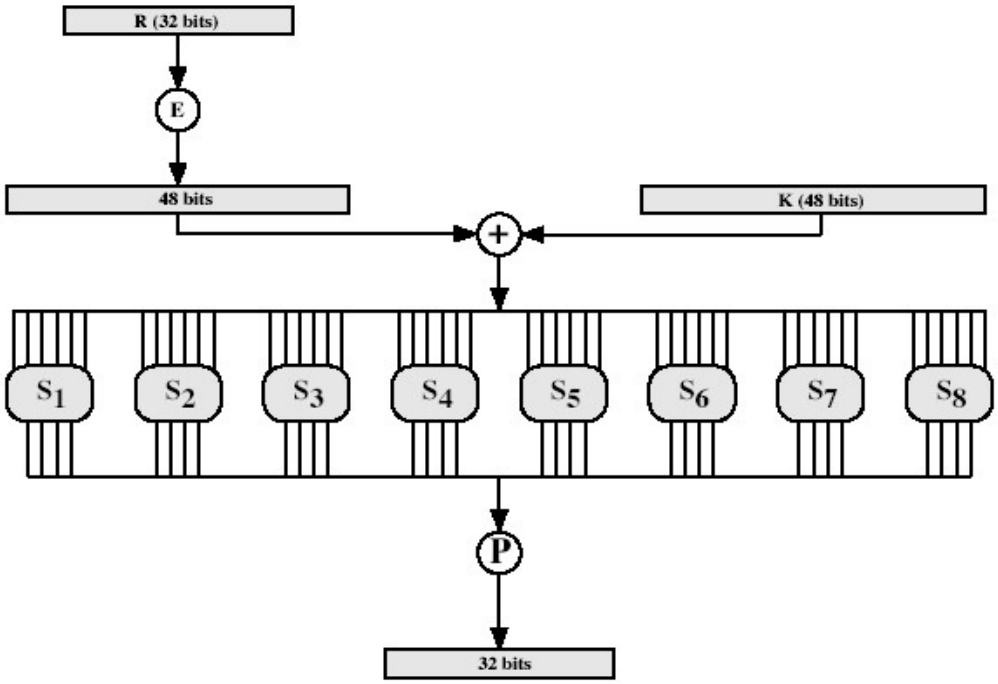
16 identical "rounds" of function application, each using different 48 bits of key

final permutation



라운드 함수

- $L_x = R_{x-1}$
- $R_x = L_{x-1} \oplus F(R_{x-1}, K_x)$,
  K_x = 라운드 x의 서브키
- F(x)



AES: Advanced Encryption Standard

- symmetric-key NIST standard, replaced DES (Nov 2001)
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

After-study Test :

1) 다음 중 메시지의 기밀성(confidentiality)를 유지하기 위한 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 디지털 서명(digital signature)
④ 메시지 해싱(hashing)

2) 다음 중 송신자의 신원(identity)을 확인하는 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 메시지 해싱(hashing)
④ 방화벽(firewall)

3) 다음 중 메시지 무결성(integrity)을 확인하는 보안 기술은?

① 암호화(encryption)
② 인증(authentication)
③ 메시지 해싱(hashing)
④ 방화벽(firewall)

4) 다음 중 시스템의 가용성(availability)를 훼손하는 공격은?

① 도청(eavesdrop)
② 가장(impersonation)
③ 하이재킹(hijacking)
④ DoS(Denial of Service)

5) 다음 중 암호화 기술에 대한 설명 중 틀린 것은?

① 대칭키 암화화(symmetric key encryption)은 1개의 키를 사용한다.
② 공개키 암호화(public key encryption)은 2개의 키를 사용한다.
③ 공개키 암호화(public key encryption)은 2개의 키를 모두 공개한다.
④ 공개키 암호화는 암호화와 복호화에서 서로 다른 키를 사용한다.

6) 다음 중 대칭키 암호화 기술이 아닌 것은?

① DES
② 3DES
③ RSA
④ AES

7) 암호에 사용된 키를 알아내기 위해 모든 경우의 수를 시도하는 공격을 무엇이라 하는가?

① 추측 공격(guessing attack)
② 사전 공격(dictionary attack)
③ 도청 공격(eavesdrop attack)
④ 전사 공격(brute force attack)