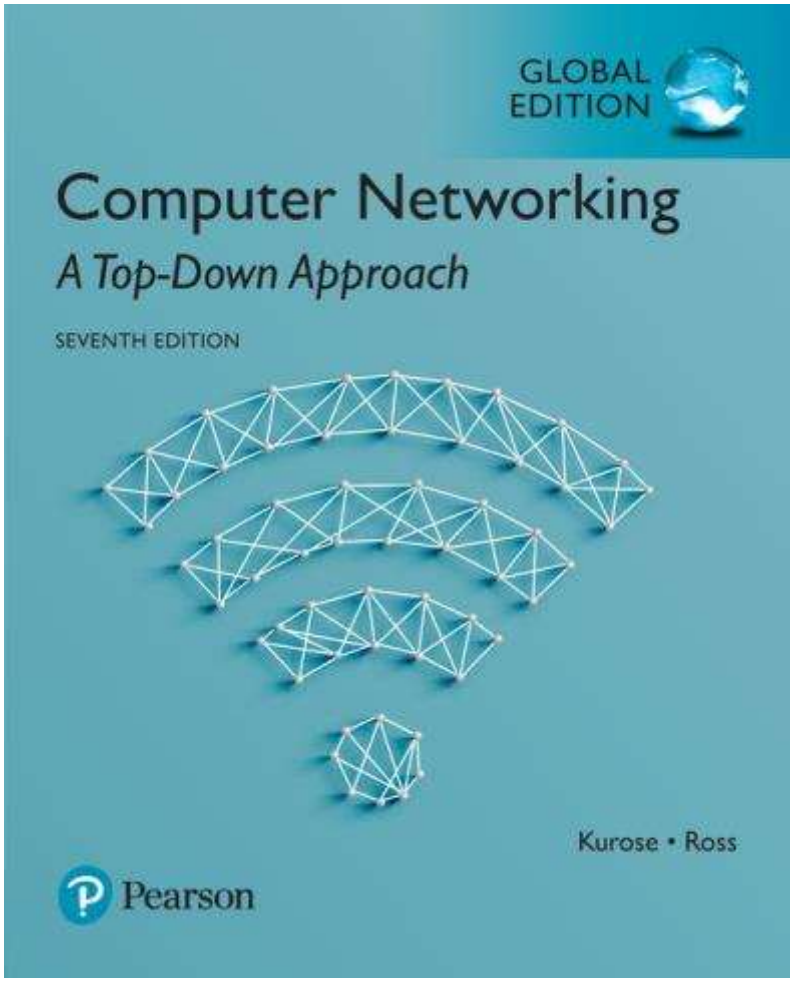
제31강
이메일 보안 프로토콜 : PGP



Computer Networking: A Top Down Approach

컴퓨터 네트워크
(2019년 1학기)

박승철교수

한국기술교육대학교
컴퓨터공학부

Pre-study Test :

1) 송신자A가 수신자B에게 이메일을 암호화하여 전송하는 과정에서 송신자가 수신자에게 암호키(대칭키)를 공개키 암호 기법을 사용하여 안전하게 전송하는 방법을 설명해보라.

2) 문제 1)의 암호 메일 전송과정에서 발생할 수 있는 중간자 공격 과정을 설명해보라.

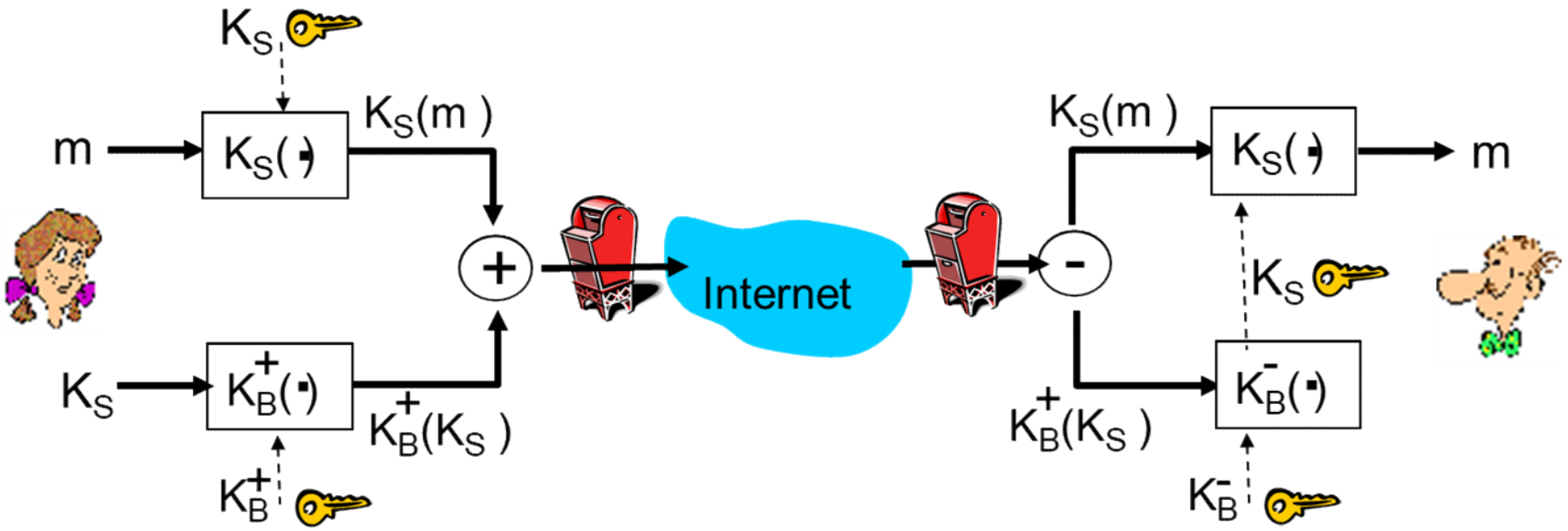
3) 송신자A가 수신자B에게 이메일을 전송하는 과정에서 메시지 무결성을 확인하는 과정을 설명해보라.

4) 송신자A가 수신자B에게 이메일을 전송하는 과정에서 수신자가 송신자를 인증할 수 있는 방법을 설명해보라.

5) 문제 4)의 송신자 인증 과정에서 발생할 수 있는 중간자 공격 과정을 설명해보라.

Secure e-mail

Alice wants to send confidential e-mail, m, to Bob.

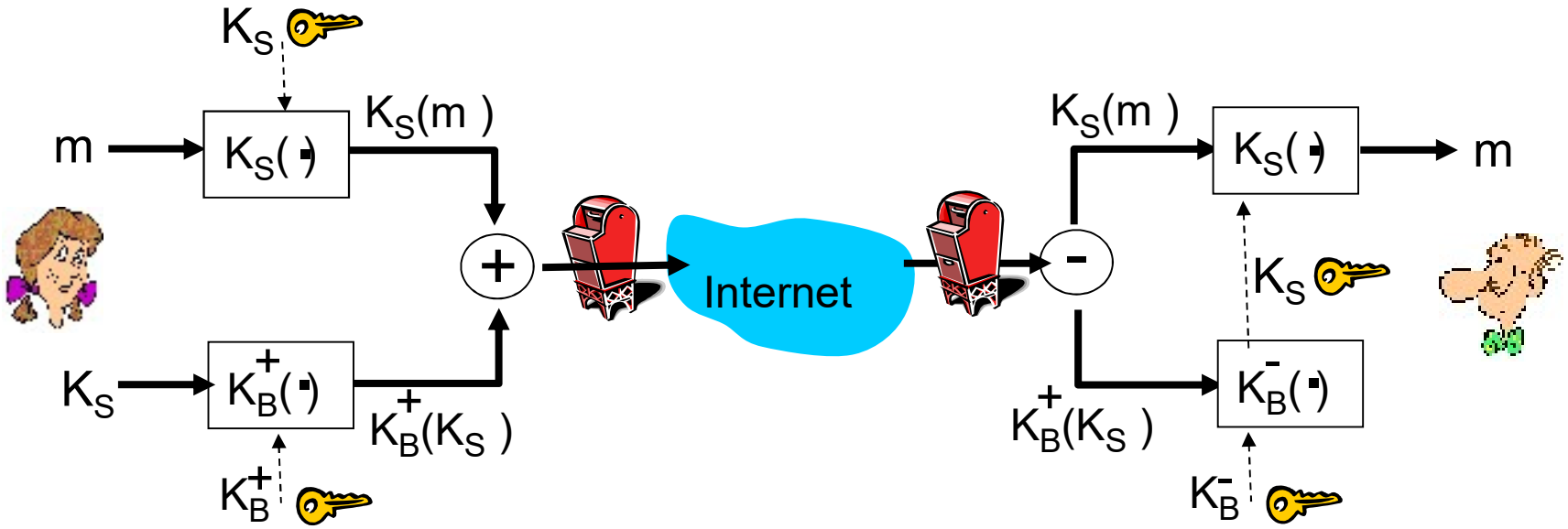


Alice:

- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob

Secure e-mail

Alice wants to send confidential e-mail, m, to Bob.

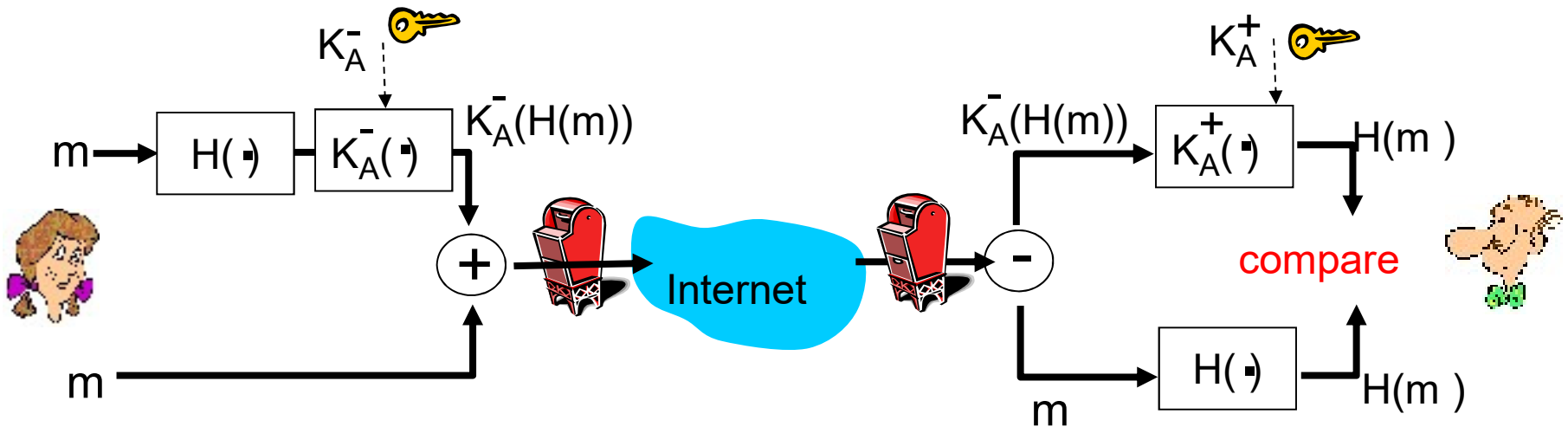


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail (continued)

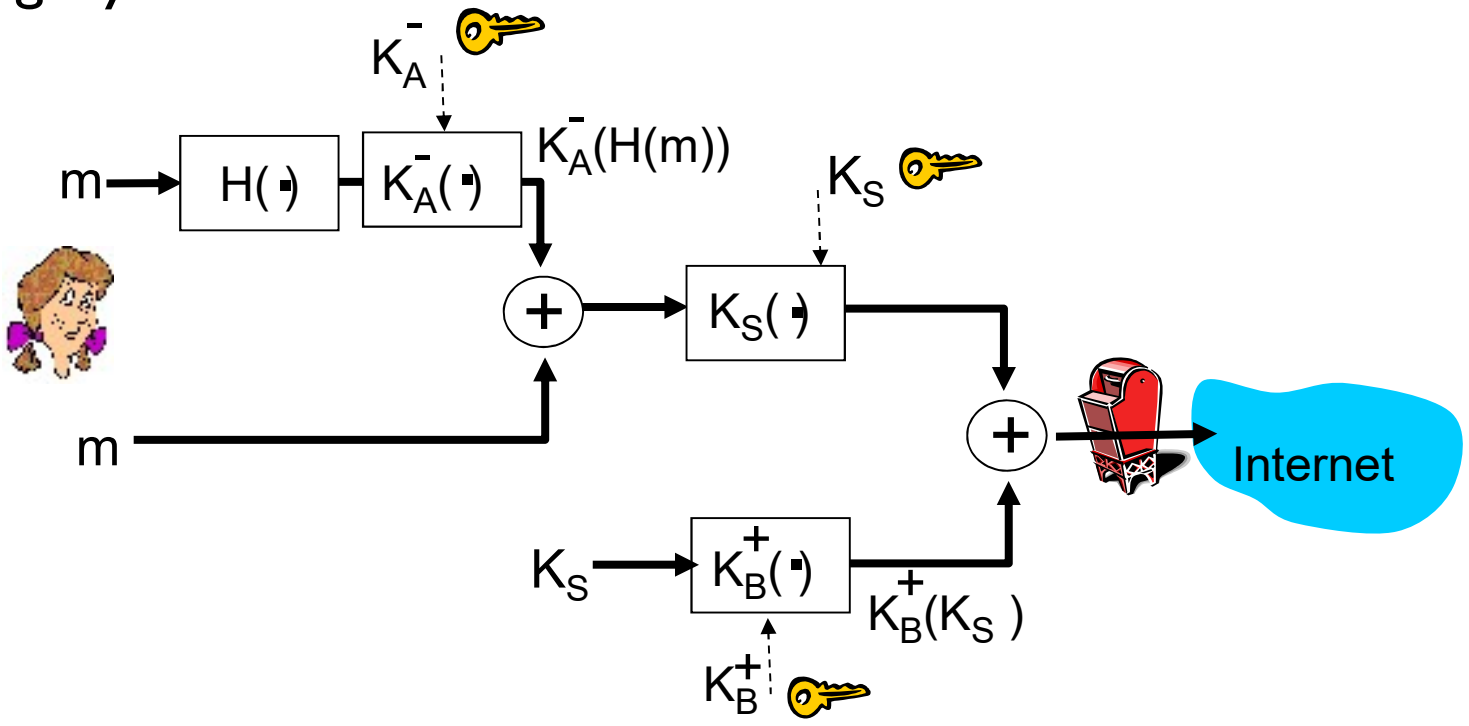
Alice wants to provide sender authentication message integrity



- Alice digitally signs message
- sends both message (in the clear) and digital signature

Secure e-mail (continued)

Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

After-study Test :

1) 송신자A가 수신자B에게 이메일을 암호화하여 전송하는 과정에서 송신자가 수신자에게 암호키(대칭키)를 공개키 암호 기법을 사용하여 안전하게 전송하는 방법을 설명해보라.

2) 문제 1)의 암호 메일 전송과정에서 발생할 수 있는 중간자 공격 과정을 설명해보라.

3) 송신자A가 수신자B에게 이메일을 전송하는 과정에서 메시지 무결성을 확인하는 과정을 설명해보라.

4) 송신자A가 수신자B에게 이메일을 전송하는 과정에서 수신자가 송신자를 인증할 수 있는 방법을 설명해보라.

5) 문제 4)의 송신자 인증 과정에서 발생할 수 있는 중간자 공격 과정을 설명해보라.