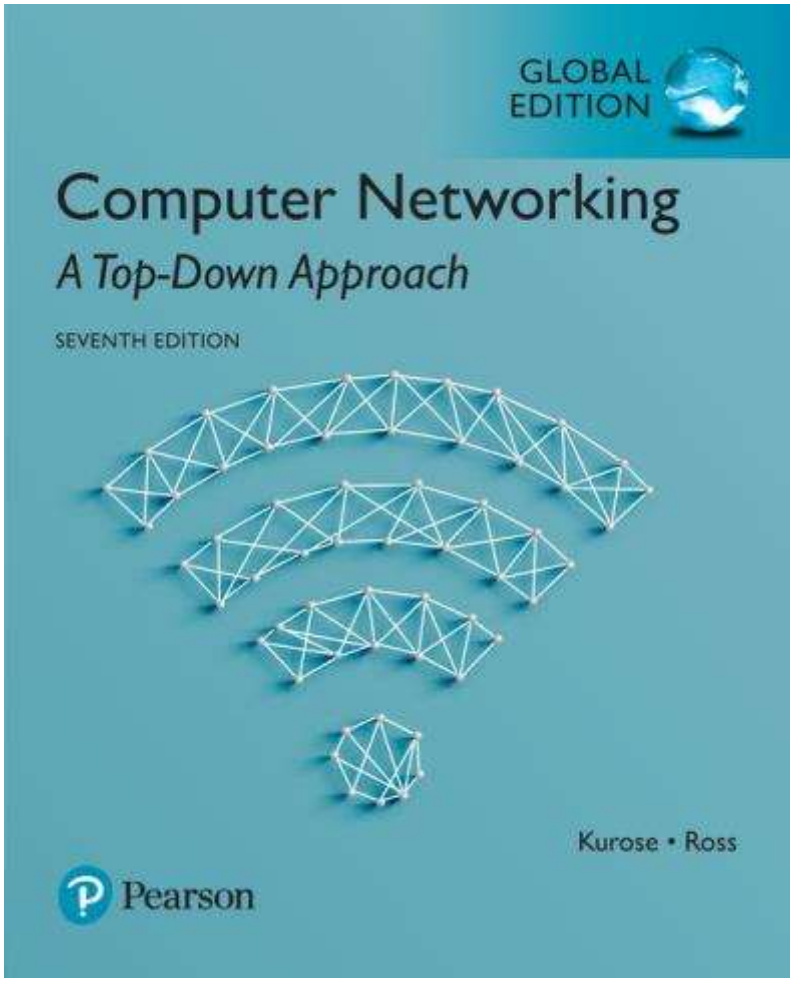
제30강
인증 프로토콜

Computer Networking: A Top Down Approach

컴퓨터 네트워크
(2019년 1학기)

박승철교수

한국기술교육대학교
컴퓨터공학부



Pre-study Test :

1) 다음 중 IP 주소를 사용한 인증을 방해하는 공격은?

① Phishing attack
② Hijacking attack
③ Spoofing attack
④ Sniffing attack

2) 다음 중 전송중인 패스워드를 가로채는 공격은?

① Phishing
② Hijacking
③ Spoofing
④ Sniffing

3) 다음 중 암호화하여 전송하는 패스워드를 무력화시키는 공격은?

① Replay attack
② Spoofing
③ Sniffing

Pre-study Test :

1) 다음 중 IP 주소를 사용한 인증을 방해하는 공격은?

① Phishing attack
② Hijacking attack
③ Spoofing attack
④ Sniffing attack

2) 다음 중 전송중인 패스워드를 가로채는 공격은?

① Phishing attack
② Hijacking attack
③ Spoofing attack
④ Sniffing attack

3) 다음 중 암호화하여 전송하는 패스워드를 무력화시키는 공격은?

① Replay attack
② Spoofing attack
③ Sniffing attack
④ DoS attack

4) 다음 중 재현 공격(replay attack)을 방어하는 기술은?

① 암호화(encryption)
② 해싱(hashing)
③ 넌스(nonce)
④ 메시지 인증 코드(MAC)

5) 다음 중 공개키를 사용하여 암호 통신을 무력화시키는 공격은?

① Replay attack
② Spoofing attack
③ Sniffing attack
④ Man-In-The-Middle attack

6) 다음 중 공개키에 대한 중간자 공격(MITM)을 방어하는 기술은?

① 암호화(encryption)
② 해싱(hashing)
③ 인증서(certificate)
④ 메시지 인증 코드(MAC)

Authentication

Goal: Bob wants Alice to "prove" her identity to him

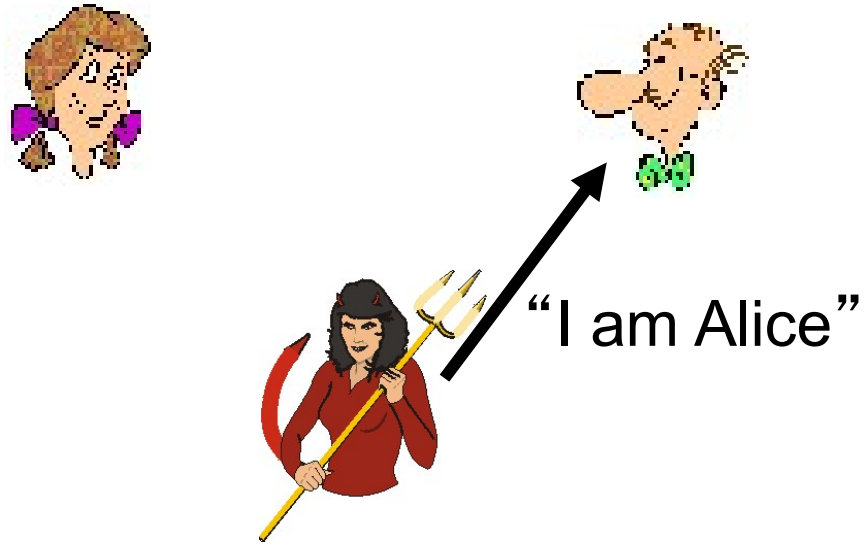
Protocol ap1.0: Alice says "I am Alice"

Failure scenario??

Authentication

Goal: Bob wants Alice to "prove" her identity to him

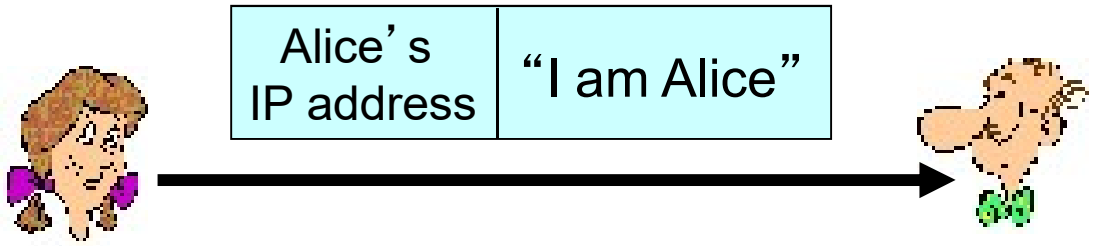
Protocol ap1.0: Alice says "I am Alice"



in a network,
Bob can not "see" Alice,
so Trudy simply declares
herself to be Alice

Authentication: another try

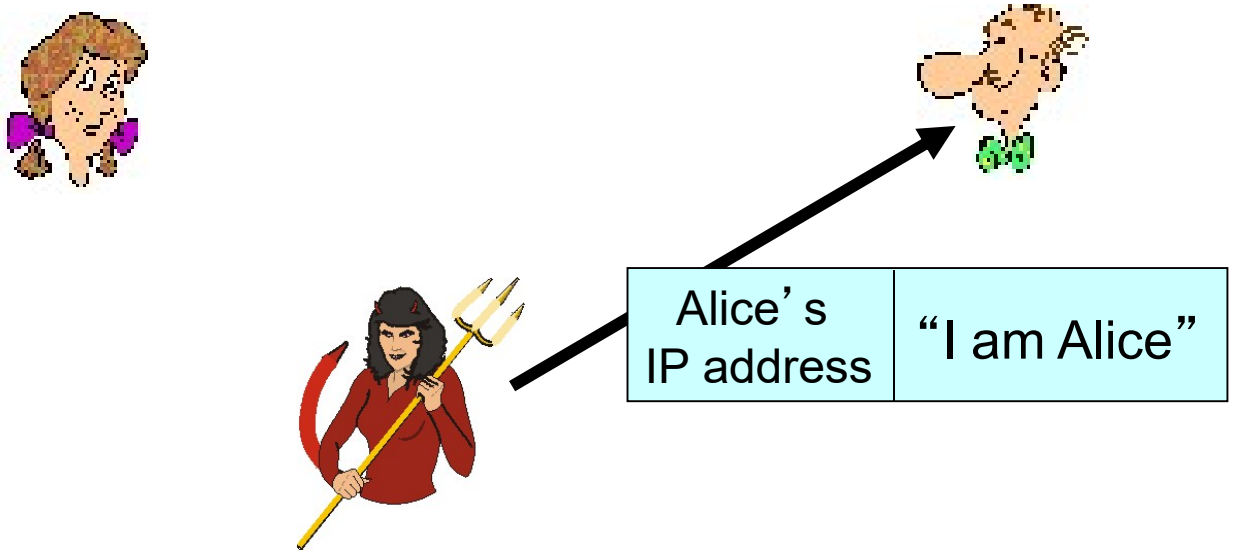
Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Failure scenario??

Authentication: another try

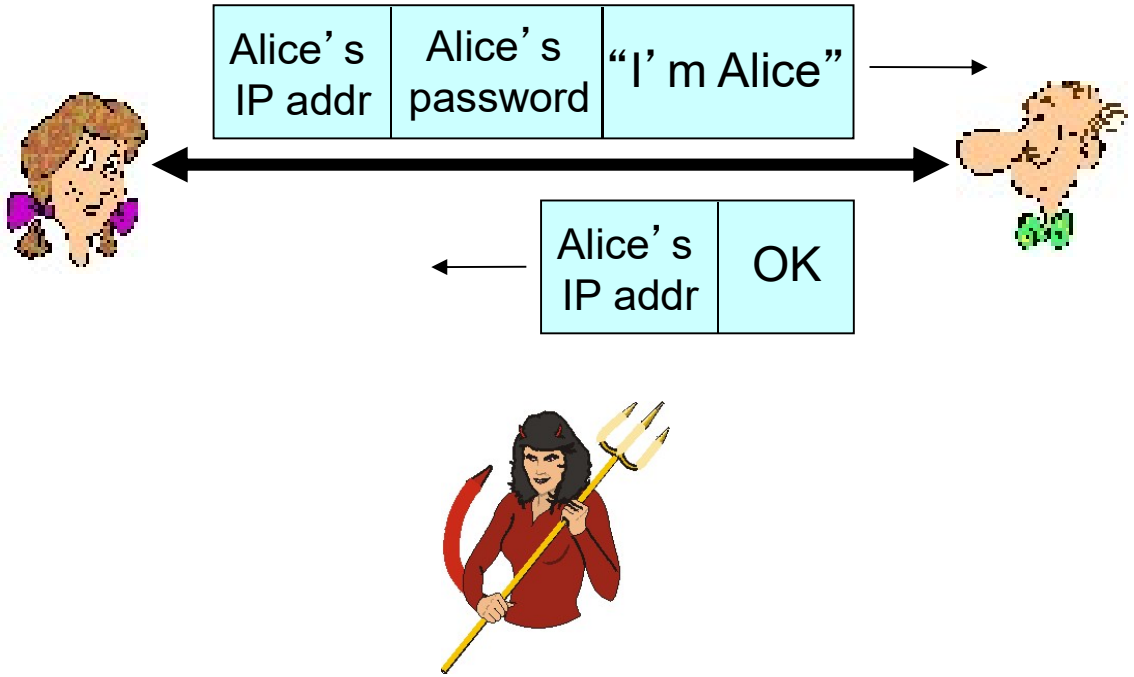
Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Trudy can create a packet "spoofing" Alice's address

Authentication: another try

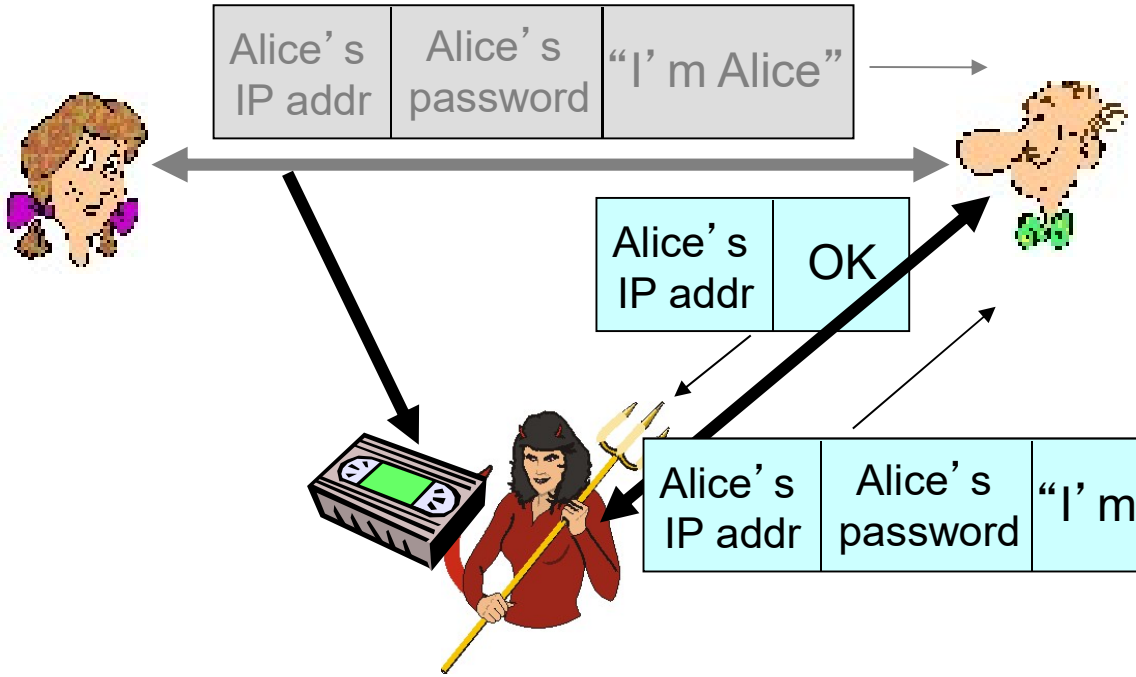
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



Failure scenario??

Authentication: another try

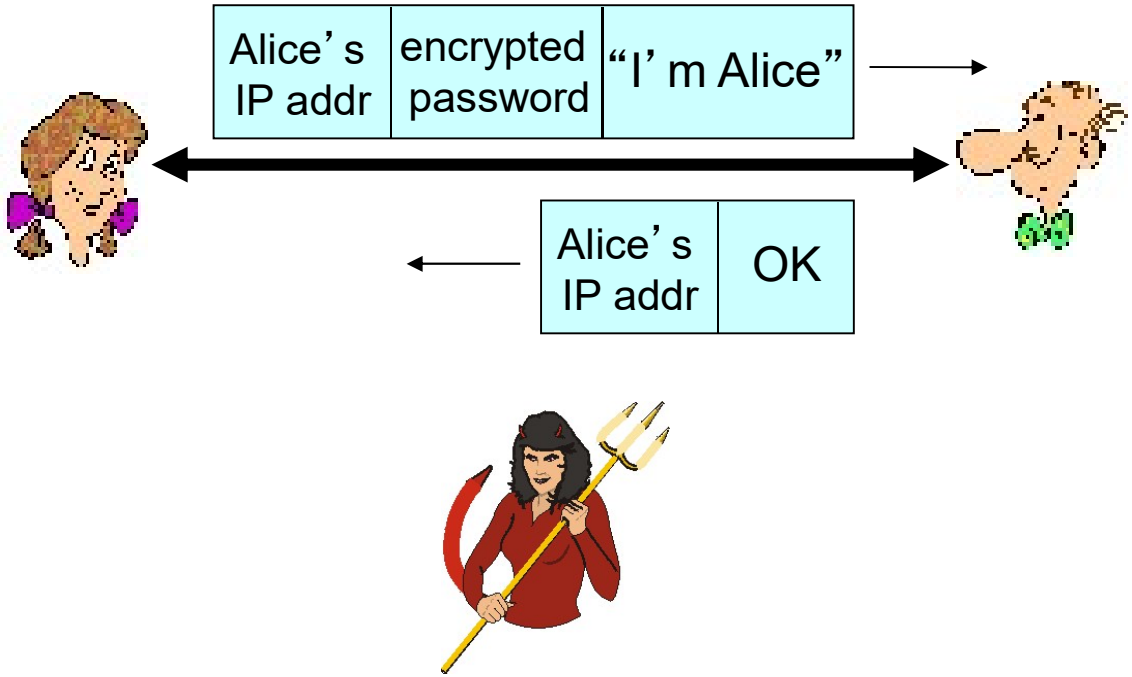
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



playback attack(재현 공격): Trudy records Alice's packet and later plays it back to Bob

Authentication: yet another try

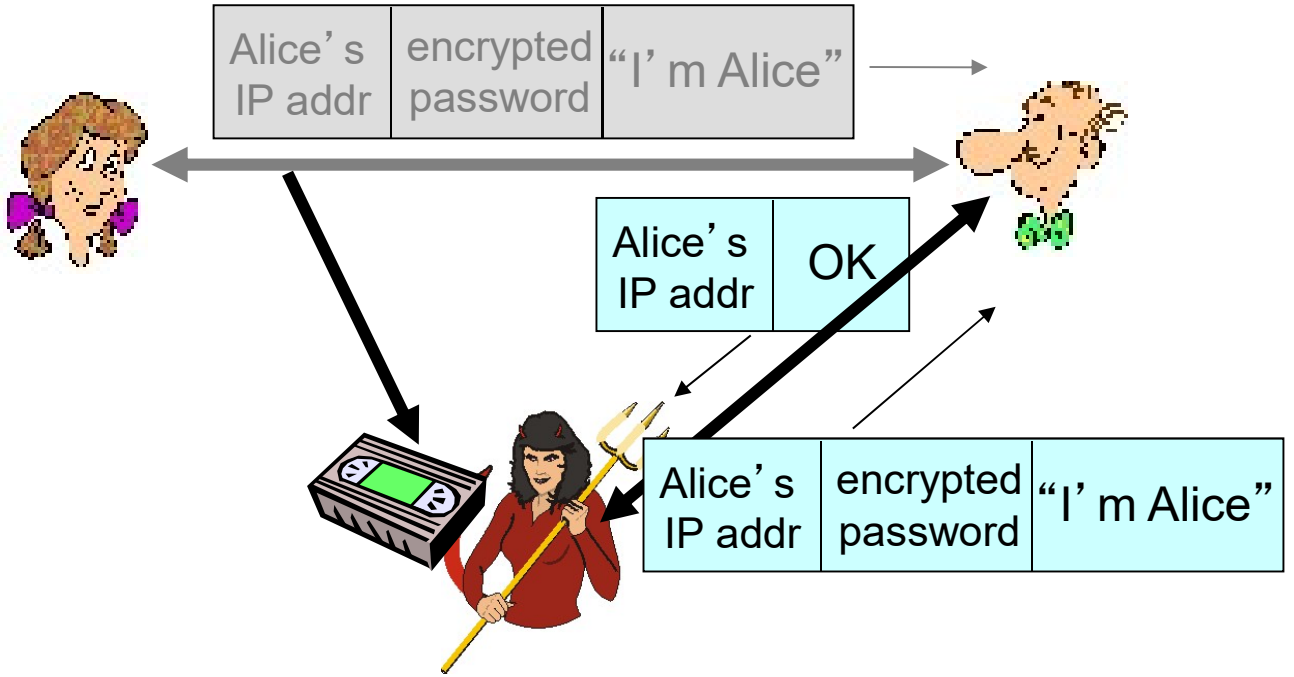
Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



문제 : 재현 공격 발생 가능성?

Authentication: yet another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



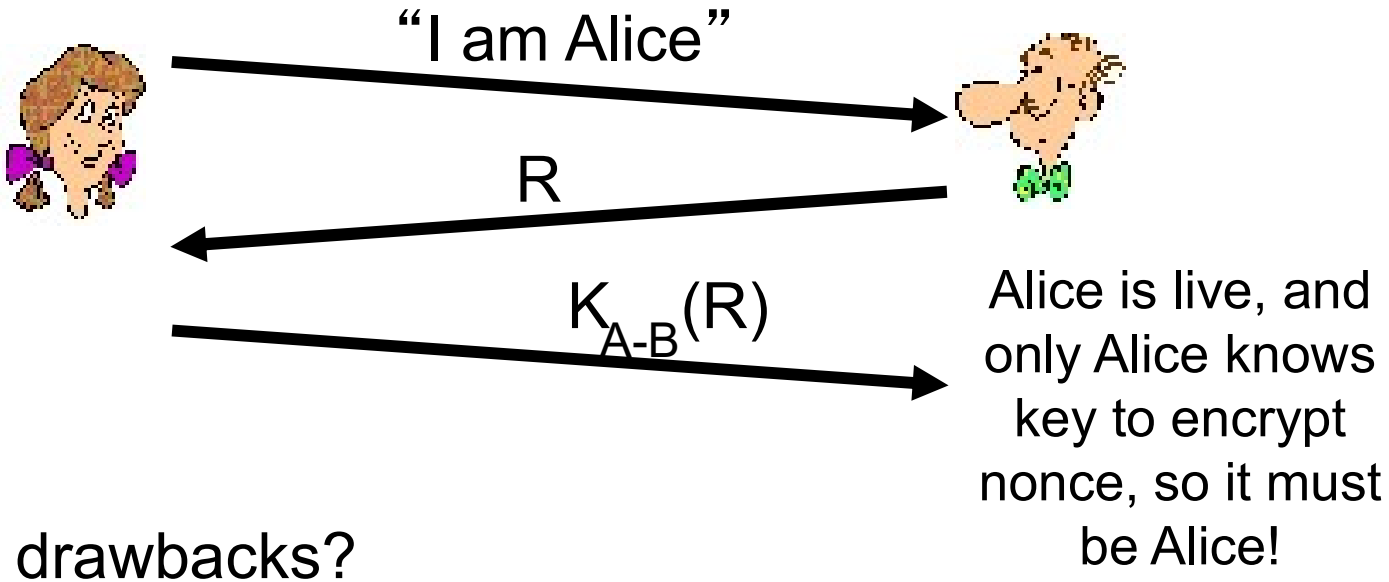
record
and
playback
still works!

Authentication: yet another try

Goal: avoid playback attack

Nonce(넌스): number (R) used only *once-in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice *nonce*, R. Alice must return R, encrypted with shared secret key



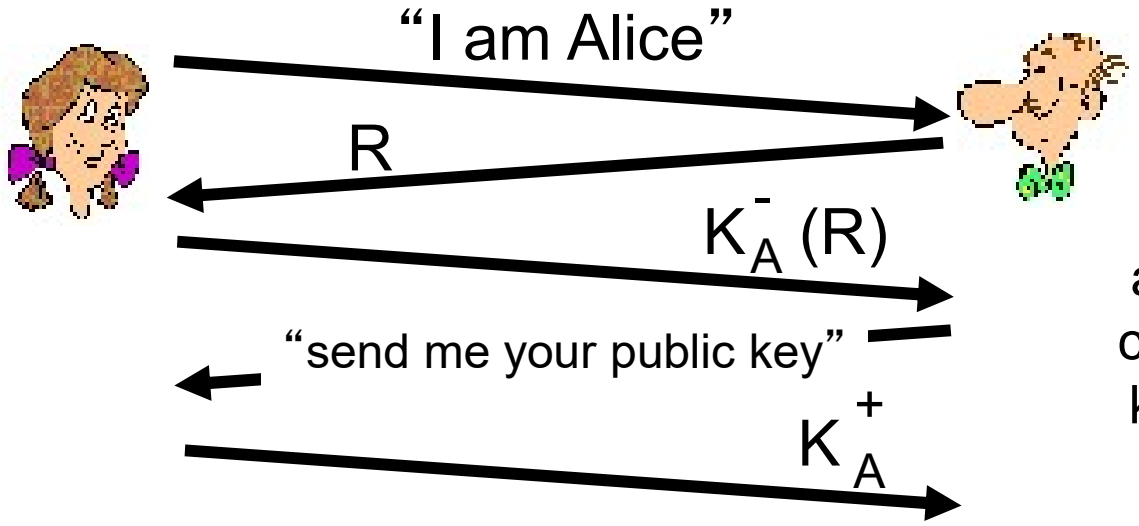
Failures, drawbacks?

Authentication: ap5.0

ap4.0 requires shared symmetric key

- can we authenticate using public key techniques?

ap5.0: use nonce(넌스), public key cryptography



Bob computes

$K_A^+(K_A^-(R)) = R$

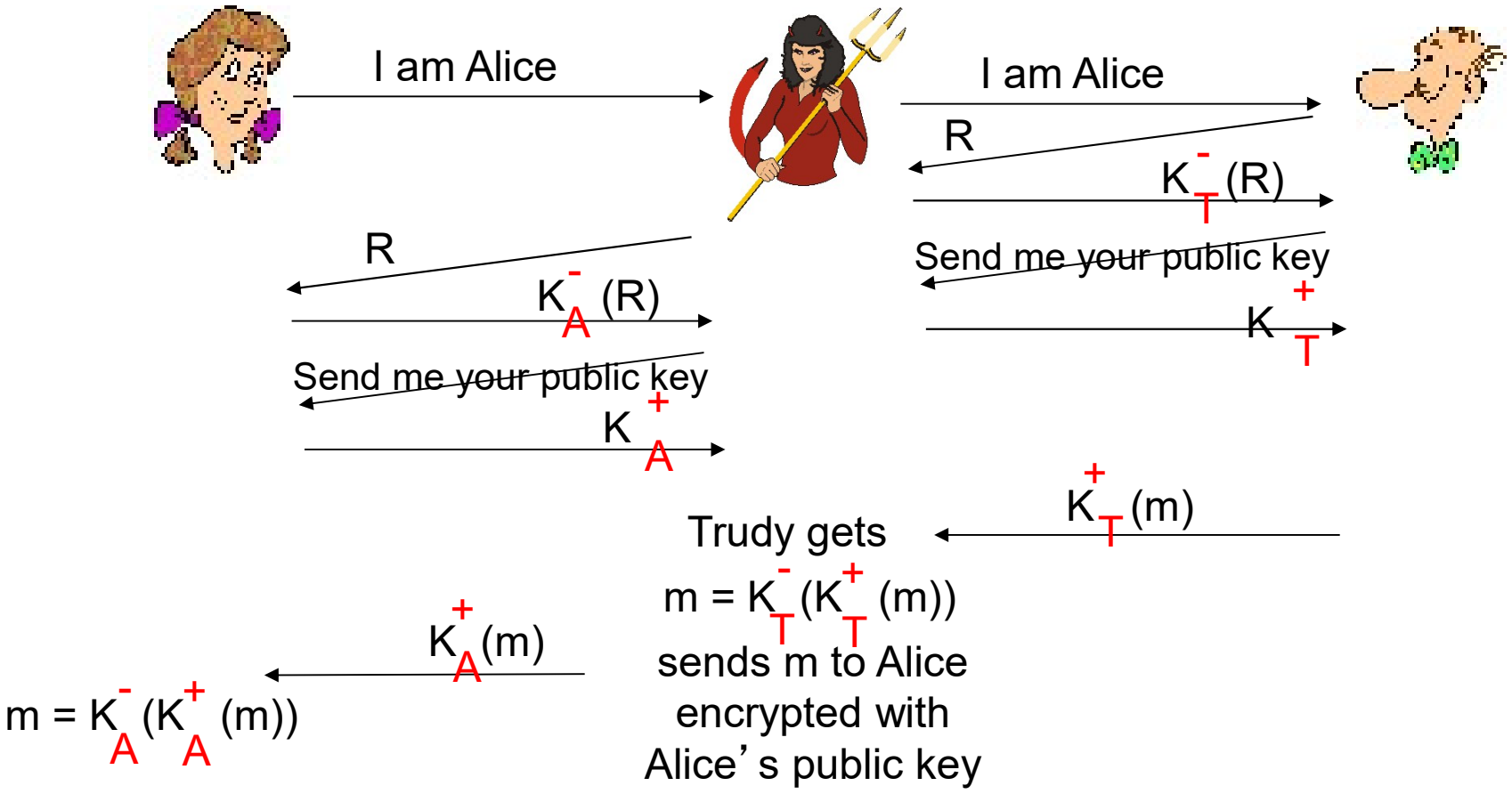
and knows only Alice could have the private key, that encrypted R such that

$K_A^+(K_A^-(R)) = R$

문제 : 인증에 실패할 경우를 설명해 보라?

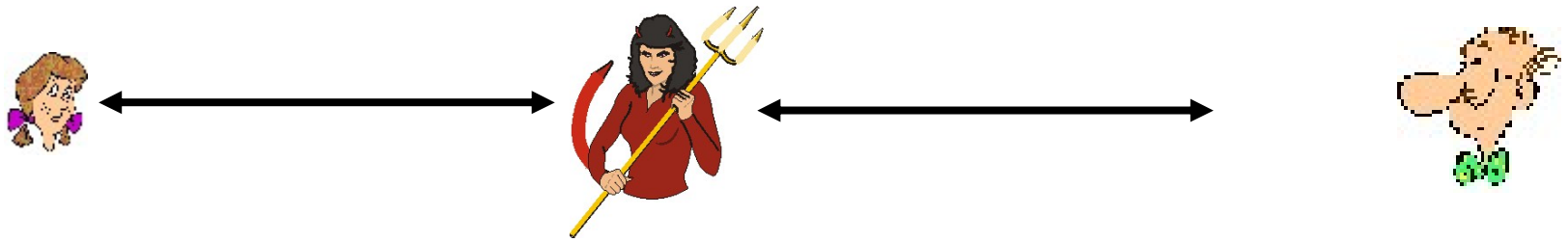
ap5.0: security hole

man (or woman) in the middle attack(중간자 공격): Trudy poses as Alice (to Bob) and as Bob (to Alice)



ap5.0: security hole

man (or woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

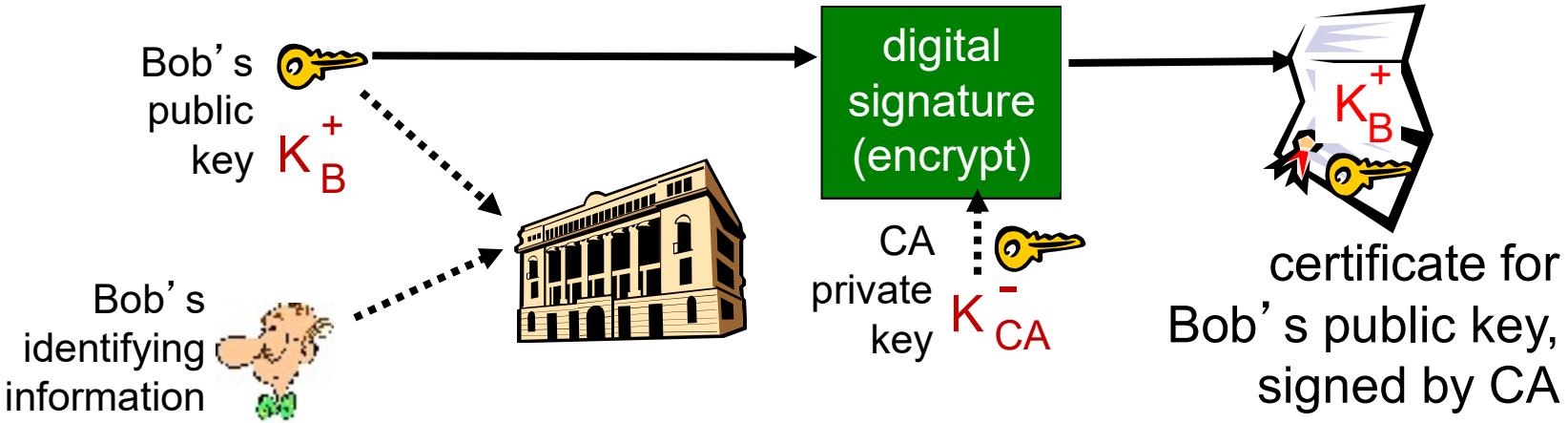


difficult to detect:

- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation!)
- problem is that Trudy receives all messages as well!

Certification authorities

- *certification authority (CA):* binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"



After-study Test :

1) 다음 중 IP 주소를 사용한 인증을 방해하는 공격은?

① Phishing attack
② Hijacking attack
③ Spoofing attack
④ Sniffing attack

2) 다음 중 전송중인 패스워드를 가로채는 공격은?

① Phishing
② Hijacking
③ Spoofing
④ Sniffing

3) 다음 중 암호화하여 전송하는 패스워드를 무력화시키는 공격은?

① Replay attack
② Spoofing
③ Sniffing

4) 다음 중 재현 공격(replay attack)을 방어하는 기술은?

① 암호화(encryption)
② 해싱(hashing)
③ 넌스(nonce)
④ 메시지 인증 코드(MAC)

5) 다음 중 공개키를 사용하여 암호 통신을 무력화시키는 공격은?

① Replay attack
② Spoofing attack
③ Sniffing attack
④ Man-In-The-Middle attack

6) 다음 중 공개키에 대한 중간자 공격(MITM)을 방어하는 기술은?

① 암호화(encryption)
② 해싱(hashing)
③ 인증서(certificate)
④ 메시지 인증 코드(MAC)