

Security II: 8.4 to 8.6

Smith College, CSC 249
April 22, 2008

slides mostly from J.F Kurose and K.W. Ross,
copyright 1996-2007

Chapter 8 roadmap

- 8.1 What is network security?
- 8.2 Principles of cryptography
- 8.3 Message integrity
- 8.4 End point authentication
- 8.5 Securing e-mail
- 8.6 Securing TCP connections: SSL
- 8.7 Network layer security: IPsec
- 8.8 Securing wireless LANs
- 8.9 Operational security: firewalls and IDS

2

So far...

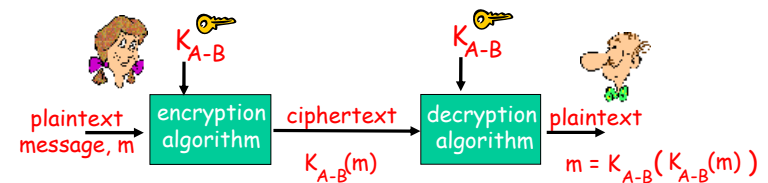
- Cryptography
- Keys - symmetric and public/private
- Hash functions

For...

- Confidentiality
- Message integrity
- Authentication ← Today

3

Symmetric key cryptography

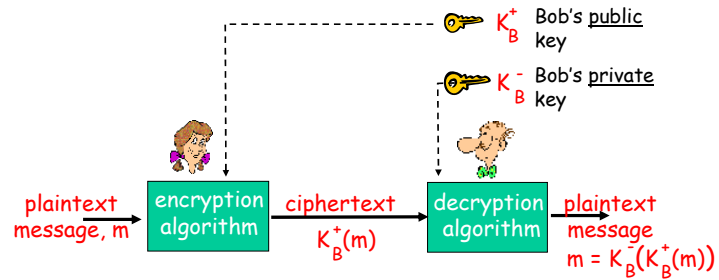


symmetric key cryptography: Bob and Alice share/know the same (symmetric) key: K

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

4

Public key cryptography



5

RSA: another important property

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

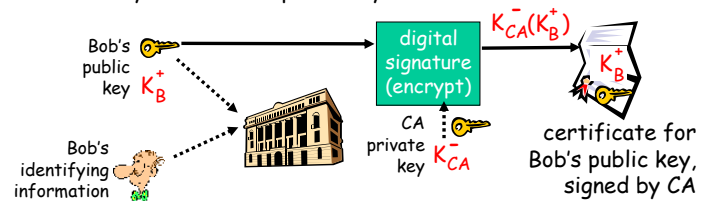
use public key first, followed by private key

use private key first, followed by public key

6

Certification Authorities

- **Certification Authority (CA):** binds public key to particular entity, E.
- E 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."



7

On To ... Authentication

8

Authentication

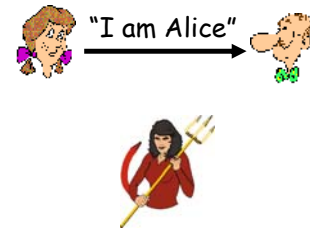
- ❑ State "I am Alice"
 - ❖ Anyone can do this
- ❑ Provide IP address along with statement
 - ❖ Easy to get someone else's IP address: "IP spoofing"
- ❑ Provide password, IP address and name
 - ❖ Playback attack
- ❑ Provide encrypted password, IP address and name
 - ❖ Playback attack still works
- ❑ Use 'nonce'
- ❑ Allow "man-in-the-middle" attacks

9

Authentication 1

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

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

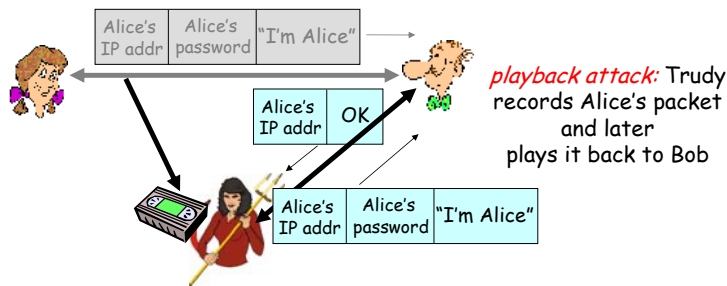


- Failure scenario??
- Including IP address help?

10

Authentication 2: Use a Password

Alice says "I am Alice" and sends her secret password to "prove" it.



11

Authentication 3: Encrypted Password

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

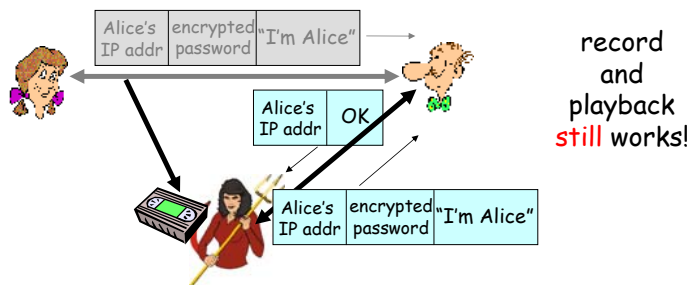


Does the playback attack **still** work?

12

Authentication 3: Encrypted Password

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



13

Activity for a Functional Authentication Protocol...

- Data to send - message or password, or session key...
- Envelopes to indicate encryption, 'sealed' with stickies
- Paired, cut-up stickies for public/private keys

14

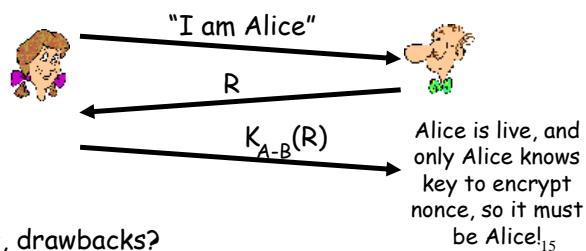
Authentication 4: yet another try

Activity: Act this out with paper, envelopes to indicate encryption & halves of stickies for public-private key pairs

Goal: avoid playback attack

Nonce: Select a 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**

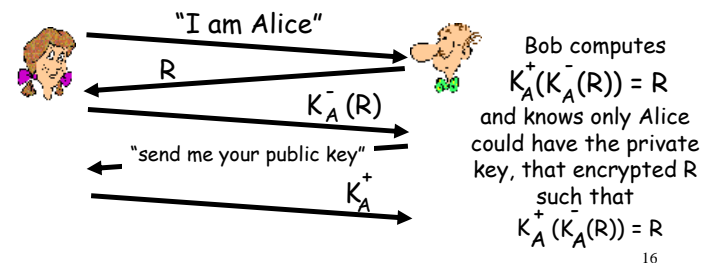


Authentication 5:

Activity: Act this out with paper, envelopes to indicate encryption & halves of stickies for public-private key pairs

- ap4.0 requires shared symmetric key
- can we authenticate using public key techniques?

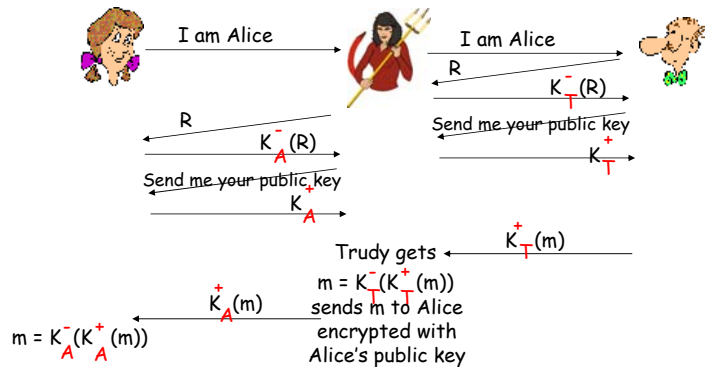
ap5.0: use nonce, **public key cryptography**



16

ap5.0: security hole

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



17

ap5.0: security hole

Man (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!

18

Chapter 8 Part 1 Recap

- Defining network security
 - ❖ confidentiality, authentication, integrity, nonrepudiation (access control)
- Cryptography
 - ❖ Symmetric, public and mixed
- Integrity
 - ❖ Message digest
 - ❖ Digital signature
- Certification Authority
- Authentication: Prove identity

19

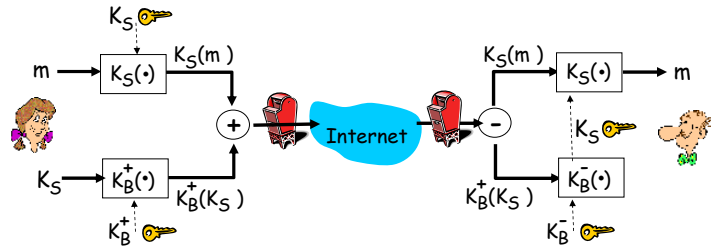
Chapter 8 roadmap

- 8.1 What is network security?
- 8.2 Principles of cryptography
- 8.3 Message integrity
- 8.4 End point authentication
- 8.5 Securing e-mail
- 8.6 Securing TCP connections: SSL
- 8.7 Network layer security: IPsec
- 8.8 Securing wireless LANs
- 8.9 Operational security: firewalls and IDS

20

Secure e-mail

- Alice wants to send confidential email to Bob
 - ❖ **Note** that this encrypted message can be tampered with, without the recipient, Bob, knowing (i.e., **there is no message integrity** here)



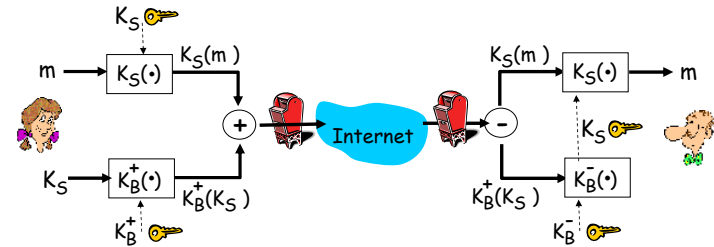
Alice:

- 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.

21

Secure e-mail

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



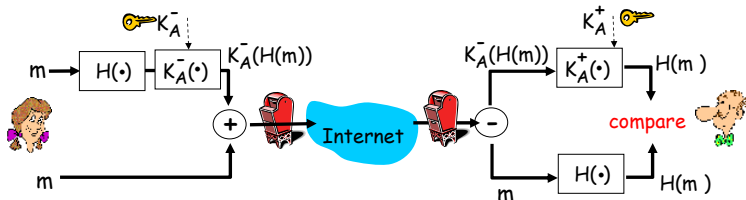
Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m
- **Note again** that there is no message integrity

22

Secure e-mail (continued)

- Alice wants to provide sender authentication & message integrity
 - ❖ **Note here** that there is no encryption of the message, m , but Bob can be sure the message has not been tampered with and that it came from Alice
 - ❖ **Also**, the hash function, $H()$, must be agreed upon beforehand

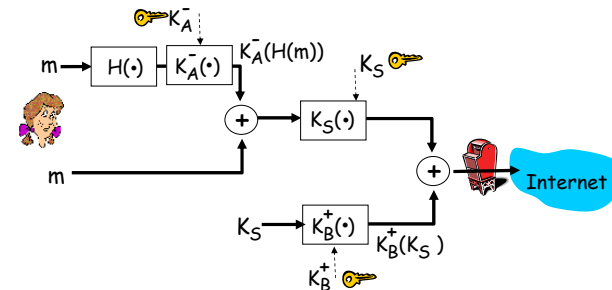


- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

23

Secure e-mail (continued)

- Alice wants it all - confidentiality, authentication & message integrity
 - ❖ Note that Alice could encrypt the entire message with her private key, **except... using the public/private keys require a lot of computation.** Creating and using a shared secret key (K_S) and encrypting this with Bob's public key (K_B^+) achieves all that Alice wants with the least computational overhead.



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

24

Pretty good privacy (PGP)

- Internet e-mail encryption scheme, de-facto standard.
- uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- provides secrecy, sender authentication, integrity.
- inventor, Phil Zimmerman, was target of 3-year federal investigation.

A PGP signed message:

```

---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
    tonight.Passionately yours,
    Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRhhGJGhg/12EpJ+1o8gE4vB3mqJ
hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
    
```

25

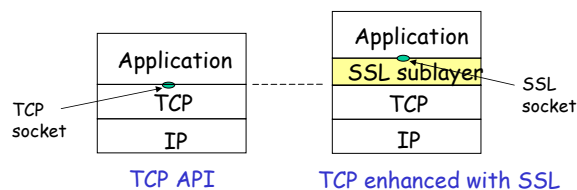
Chapter 8 roadmap

- 8.1 What is network security?
- 8.2 Principles of cryptography
- 8.3 Message integrity
- 8.4 End point authentication
- 8.5 Securing e-mail
- 8.6 Securing TCP connections: SSL
- 8.7 Network layer security: IPsec
- 8.8 Securing wireless LANs
- 8.9 Operational security: firewalls and IDS

26

Secure sockets layer (SSL)

- provides transport layer security to any TCP-based application using SSL services.
 - e.g., between Web browsers, servers for e-commerce (shttp)
- security services:
 - server authentication, data encryption, client authentication (optional)

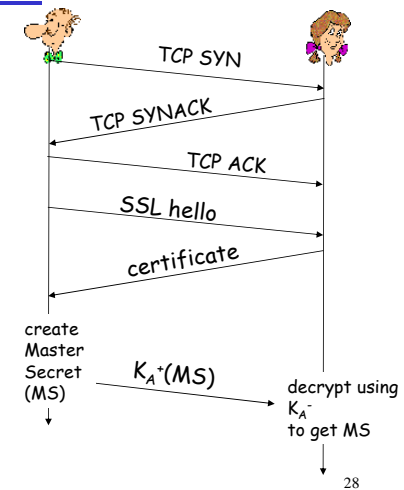


27

SSL: three phases

1. Handshake:

- Bob establishes TCP connection to Alice
- authenticates Alice via CA signed certificate
- creates, encrypts (using Alice's public key), sends master secret key to Alice
 - nonce exchange not shown



28

SSL: three phases

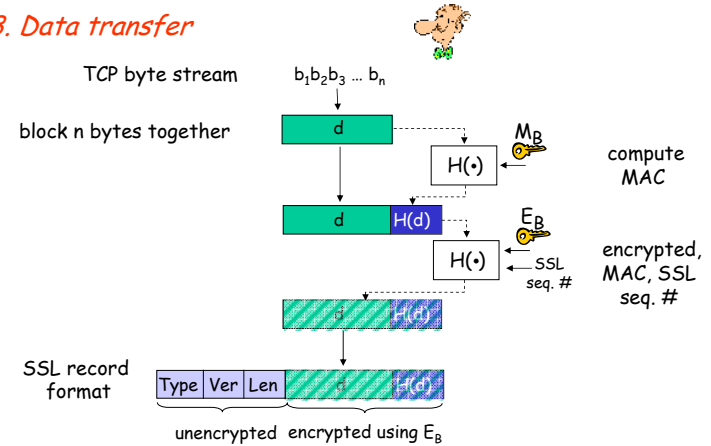
2. Key Derivation:

- Alice, Bob use shared secret (MS) to generate 4 keys:
 - ❖ E_B : Bob→Alice data encryption key
 - ❖ E_A : Alice→Bob data encryption key
 - ❖ M_B : Bob→Alice MAC key (message authentication code)
 - ❖ M_A : Alice→Bob MAC key
- encryption and MAC algorithms negotiable between Bob, Alice
- Why 4 keys? ... This is a good thing to know!

29

SSL: three phases

3. Data transfer



30

Network Security (summary)

Basic techniques.....

- ❖ cryptography (symmetric and public)
- ❖ message integrity
- ❖ end-point authentication

.... used in many different security scenarios

- ❖ secure email
- ❖ secure transport (SSL)

Operational Security: firewalls and IDS

31