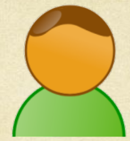





Security 2

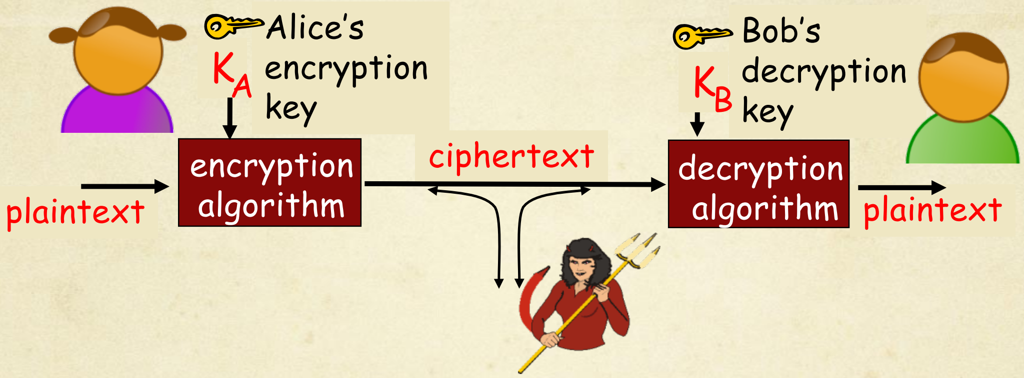
CSC 249
April 12, 2018

Network Security

- Recap Message Integrity and Authentication
- Trusted Intermediaries
- Secure email – pretty good privacy (PGP)

2

Cryptographic Keys



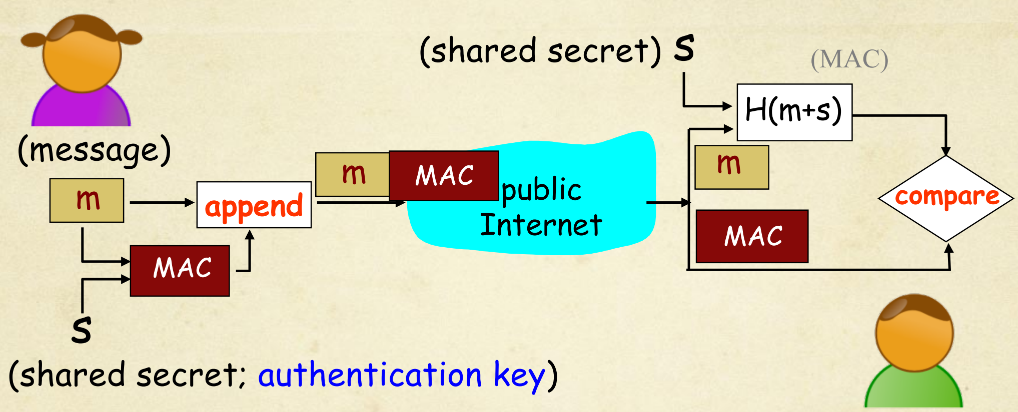
Symmetric key cryptography: sender & receiver keys are *identical* and *secret* (known by the two parties)

Public-key cryptography: one key is *public*, and the other key is *secret*, and know only by one party

3

(1) Message Authentication Code:

→ Use Shared Secret: H(m+s) = MAC



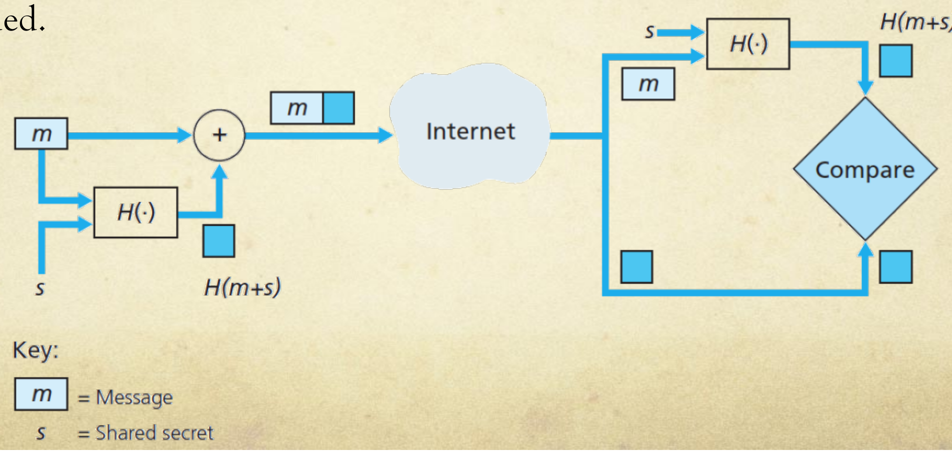
Issues

→ How to distribute the shared authentication key, s

→ Prevents Trudy sending {m', H(m')} and Bob not know

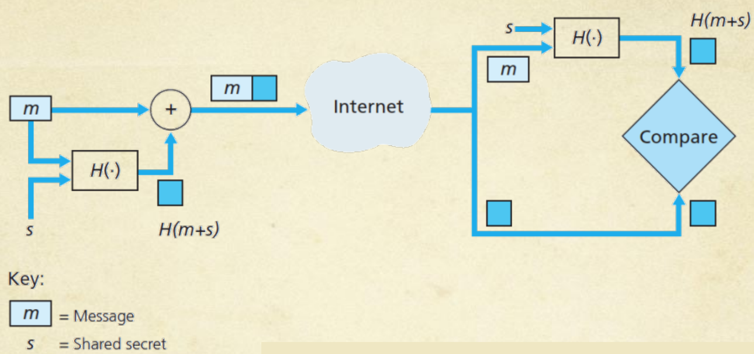
Task: Integrity + Authentication

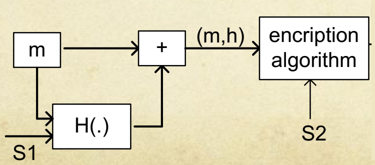
- Suppose Alice and Bob share **two** secret keys:
  - an authentication key S1 and
  - a symmetric encryption key S2.
- Augment the figure so that both integrity and confidentiality are provided.



6

Solution: Integrity + Authentication

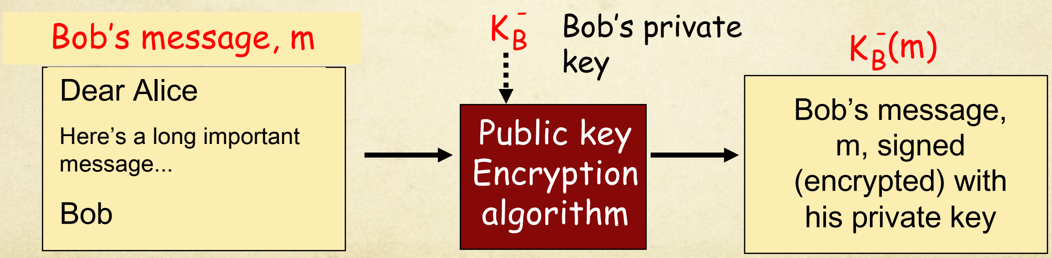




7

(2) Digital Signature: Use Public Key Cryptography

- Bob signs ***m*** by encrypting it with his private key K_B^-, creating "signed" message, $K_B^-(m)$
- Binds the message to the sender (stronger than H(m+s))



9

* End point authentication *

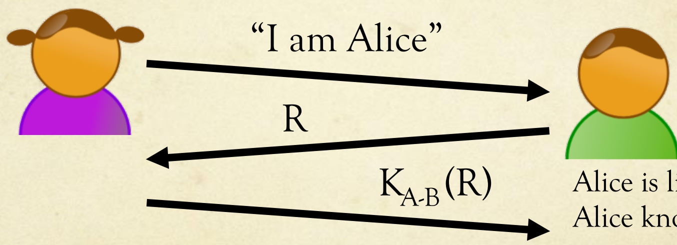
1) State "I am Alice"
   - Anyone can do this
2) Provide IP address along with statement
   - Easy to get and use someone else's IP address: "IP spoofing"
3) Provide password, IP address and name
   - Playback attack
   - Provide encrypted password, IP address and name → Playback attack still works
4) Use 'nonce' (think about Apple Pay)
   - A '**n**umber' used only '**once**'
   - Allows for "woman-in-the-middle" attacks

10

Authentication: avoid playback attack

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

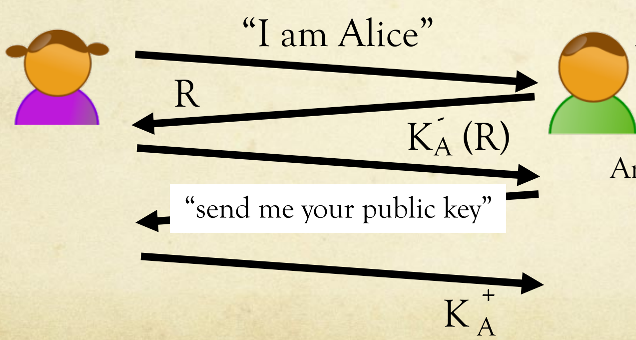
To prove Alice is "live", Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice

Authentication with Nonce

- Able to authenticate using public key techniques?
- Use nonce *and* public key cryptography?
- Failures or drawbacks?



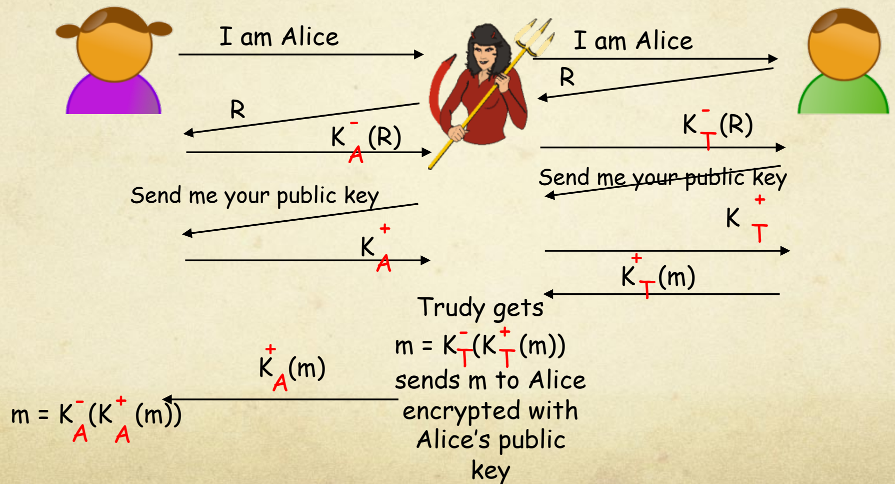
Bob computes
$K_A^+(K_A^-(R)) = R$

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

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

‘nonce’ Security Hole

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



15

‘nonce’ Security Hole

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.
  - ❑Bob, Alice can meet one week later and recall conversation)
- ❑ Problem is that Trudy receives all messages as well

16

* Trusted Intermediaries *

Symmetric key problem:

- How do two entities establish shared secret key over network?

Solution:

- Trusted **K**ey **D**istribution **C**enter (KDC) acting as intermediary between entities

Public key problem:

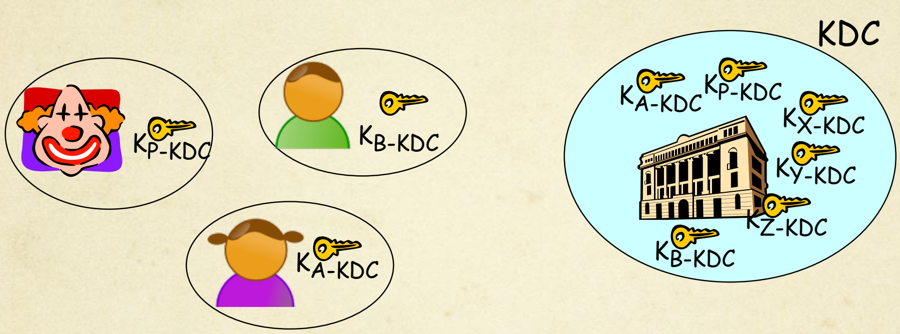
- How do you know you are getting the actual public key and not the public key of an intruder?

Solution:

- trusted **C**ertification **A**uthority (CA)

17

Key Distribution Center (KDC)



18

KDC Question – on Handout

- Explore how the session key can be distributed- without public key cryptography- using a Key Distribution Center (KDC).
- The KDC is a server that shares a unique secret symmetric key with each registered user.
- For Alice and Bob, denote these keys by $K_{A\text{-}KDC}$ and $K_{B\text{-}KDC}$.
- Design a scheme that uses the KDC to distribute K_s to Alice and Bob.
- Use three messages to distribute the session key:

(i) a message from Alice to the KDC

(ii) a message from the KDC to Alice

(iii) a message from Alice to Bob.

21

KDC Question Continued

- Design a scheme that uses the KDC to distribute K_s to Alice and Bob.
- Use three messages to distribute the session key:

(i) a message from Alice to the KDC

(ii) a message from the KDC to Alice

(iii) a message from Alice to Bob.

- The first message is $K_{A\text{-}KDC}$ (A, B).
  - Using the notation, $K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$, K_s, A and B
  - Diagram the following questions.
  - 'A' and 'B' denote identifiers – IP addr? - for Alice & Bob
  - Show the second message on the diagram
  - Show the third message on a diagram

22

Public Key Certification

<u>public key problem:</u>

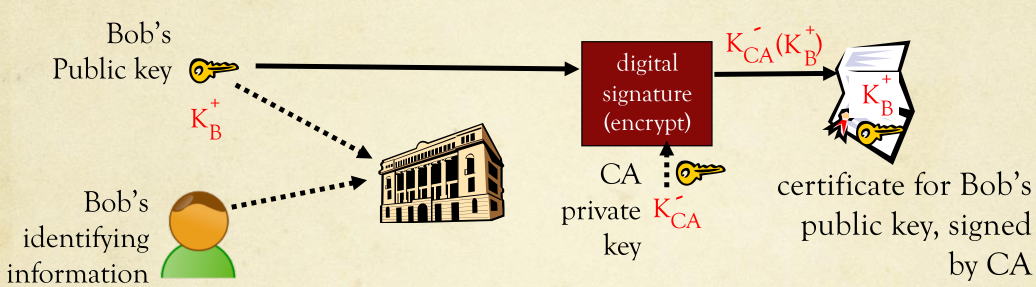
- When Alice obtains Bob's public key (from website, e-mail ...), how does she *know* it is Bob's public key, not Trudy's?

solution:

- trusted certification authority (CA)

23

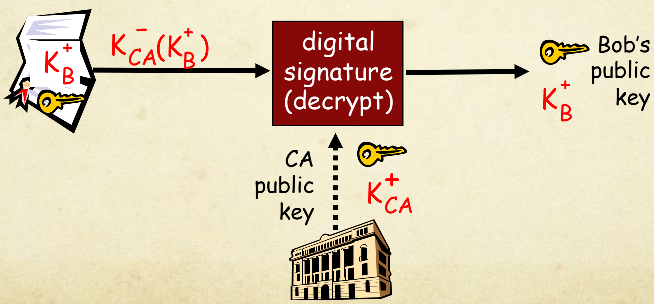
Certification Authorities



24

Certification Authorities

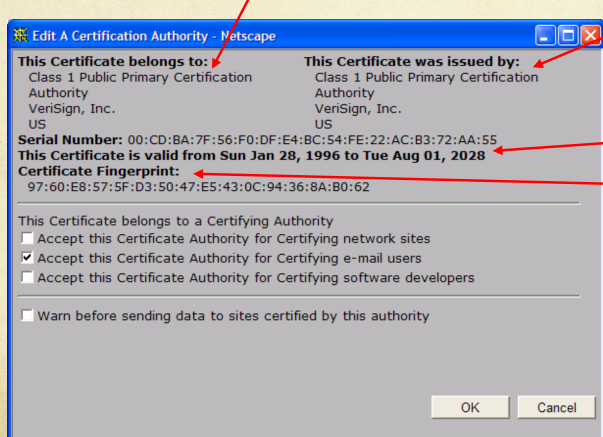
- When Alice wants Bob's public key:
  - get Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



26

A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)


Edit A Certification Authority - Netscape

This Certificate belongs to:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US

This Certificate was issued by:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US

Serial Number: 00:CD:BA:7F:56:F0:DF:E4:BC:54:FE:22:AC:B3:72:AA:55
This Certificate is valid from Sun Jan 28, 1996 to Tue Aug 01, 2028
Certificate Fingerprint:
97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62

This Certificate belongs to a Certifying Authority
- [ ] Accept this Certificate Authority for Certifying network sites
- [x] Accept this Certificate Authority for Certifying e-mail users
- [ ] Accept this Certificate Authority for Certifying software developers

- [ ] Warn before sending data to sites certified by this authority

OK Cancel

- info about certificate issuer
- valid dates
- digital signature by issuer

27

Discussion Question

- If a Key Distribution Center goes down, what is the impact on the ability of parties to communicate securely. Who can and cannot communicate?
- If a Certification Authority goes down, what is the impact on the ability of parties to communicate securely. Who can and cannot communicate?

28

Recap so far...

Security mechanisms

- Cryptography
  - Keys – symmetric and public/private
  - Key distribution & Certificates
- Hash function + Authentication key
- Nonce

To provide

- Secure access to resources
- Confidentiality
- Message integrity
- Authentication

Security Mechanisms

	Identify elements	Define how it works	Identify weaknesses
Password			
Symmetric key cryptography			
Public key cryptography			
Message Authentication Code, MAC			
Digital signature			
Nonce			
Key distribution center			
Certificate authority			

Which mechanisms address which principles?

	Access to Resources	Confidentiality	Data/Message Integrity	Authentication
Password				
Symmetric key cryptography				
Public key cryptography				
Message Authentication Code, MAC				
Digital signature				
Nonce				
Key distribution center				
Certificate authority				

Review: Network Security

- The field of network security is about:
  - How computer networks can be attacked
  - How to defend networks against these attacks
  - How to design protocols and hardware that are immune to attacks
  - Security considerations are in all layers
  - Internet protocol designers are trying to catch up

Chapter 8 So Far

- Defining network security
  - confidentiality, authentication, integrity, nonrepudiation (access control)
- Cryptography
  - Symmetric, public and mixed
- Integrity
  - Message digest
  - Digital signature
- Certification Authority & KDC