CS 312
Internet Concepts

Applications & Application-Layer Protocols: Securing the Web

Dr. Michele Weigle
Department of Computer Science
Old Dominion University
mweigle@cs.odu.edu

http://www.cs.odu.edu/~mweigle/CS312-F08/

HTTPS

- Hypertext Transfer Protocol over Secure Socket Layer, the secure version of HTTP
  - » Netscape Communications Corporation
  - » Encrypts the session data
    - ❖ Using either the SSL (Secure Socket Layer) protocol or the TLS (Transport Layer Security) protocol
  - » SSL and TLS work above TCP but below HTTP, FTP, SMTP, etc. application protocols

Refrence:
http://en.wikipedia.org/wiki/HTTPS

HTTPS

- Transferred using HTTP, encrypted
  - » with default TCP/IP port 443
- For Web pages, the URL begins with https://
- Provides authentication and encrypted communication
  - » authentication
    - ❖ to confirm the sender being the true claimed,
    - ❖ e.g. using digital certificate by trusted third party (TTP)
  - » encryption-decryption
    - ❖ using a cipher (encryption-decryption algorithm)
    - ❖ with symmetric or asymmetric (related public and private) keys

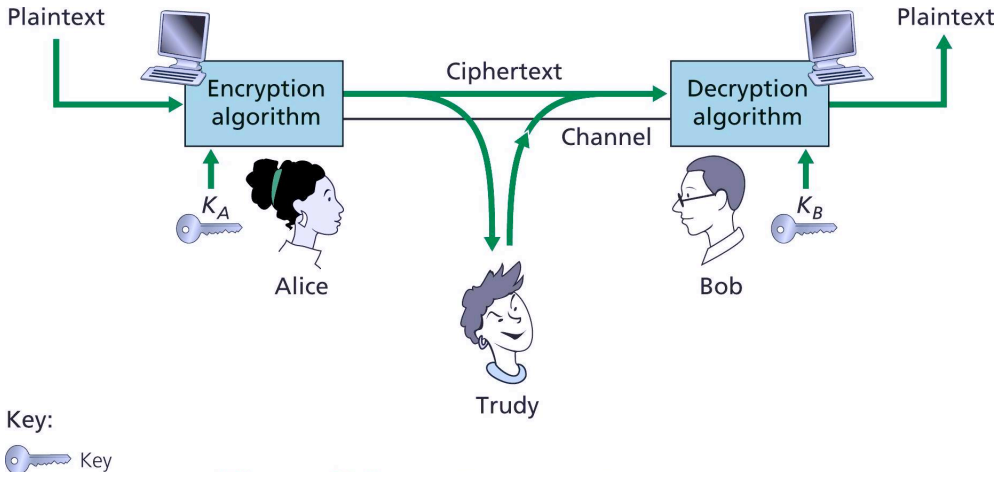
Encryption and Decryption

- Symmetric cryptography
  - » Same key for encryption and decryption
    - ❖ would be efficient as long as the key is pre-agreed and secure
  - » Not suitable for the Web
- Asymmetric-key cryptography (also called Public -key cryptography)
  - » Using a pair of related public and private keys. Encryption and decryption are asymmetric.
  - » Used in HTTPS

Principles of Cryptography

The language of cryptography

"crypto" - secret
"graphy" - writing



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret*

Principles of Cryptography

Symmetric key cryptography

Substitution cipher: substituting one thing for another

» Caesar cipher: substitute one letter for another by shifting alphabet *k* letters

```
plaintext:  abcdefghijklmnopqrstuvwxyz
ciphertext: lmnopqrstuvwxyzabcdefghijk
```

E.g.: `Plaintext: bob. i love you. alice`

`ciphertext: mzm. t wzgp jzf. lwtnp`

Principles of Cryptography

Symmetric key cryptography

Substitution cipher: substituting one thing for another

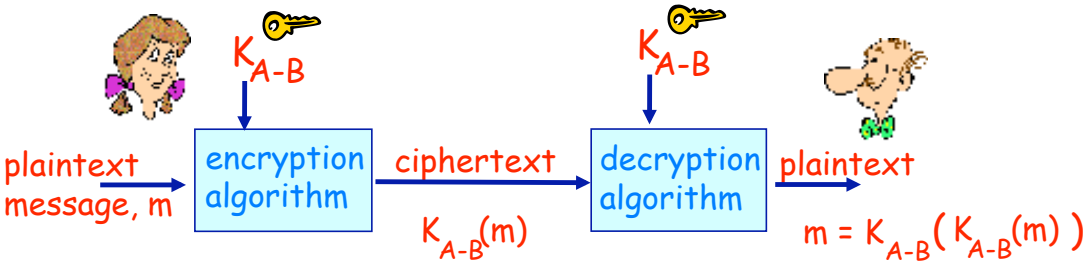
» monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
             |                       |
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

E.g.: `Plaintext: bob. i love you. alice`
`ciphertext: nkn. s gktc wky. mgsbc`

Principles of Cryptography

Symmetric key cryptography



Symmetric key crypto: Bob and Alice know same key, K_{A-B}

E.g.: Key is knowing substitution pattern in monoalphabetic substitution cipher

Principles of Cryptography

Public Key Cryptography

symmetric key cryptography

» requires sender, receiver know shared secret key

public key cryptography

» radically different approach

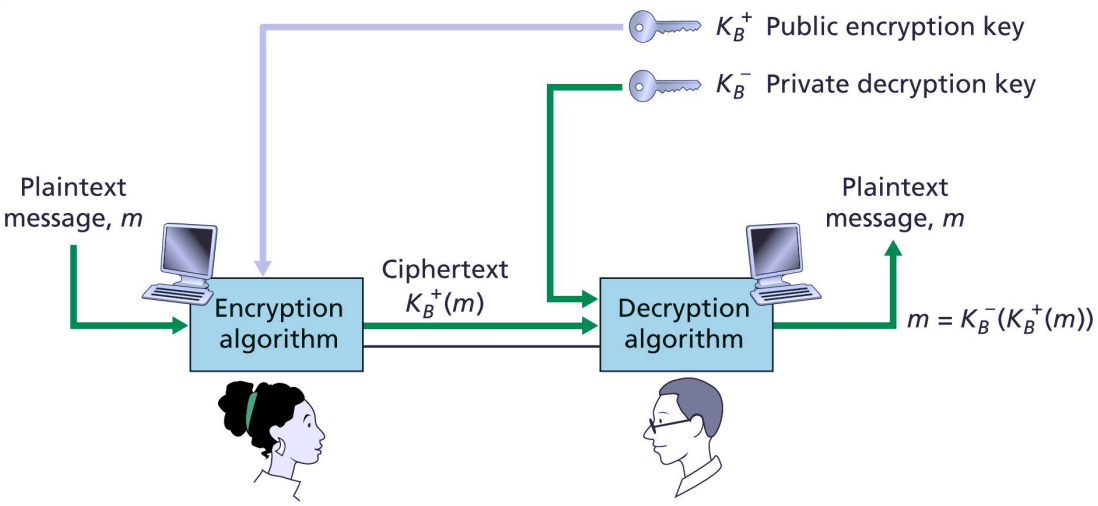
» sender, receiver do not share secret key

» public encryption key known to all

» private decryption key known only to receiver

Principles of Cryptography

Public Key Cryptography



Public Key Cryptography Algorithms

Requirements

Need $K^+_B(m)$ and $K^-_B(m)$ such that

1. $K^-_B(K^+_B(m)) = m$
2. Given public key K^+_B, it should be impossible to compute private key K^-_B

RSA: **R**ivest, **S**hamir, **A**delson algorithm

RSA

Another Important Property

The following property will be *very* useful later:

$$\underbrace{K^-_B(K^+_B(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K^+_B(K^-_B(m))}_{\text{use private key first, followed by public key}}$$

Result is the same!

Public Key Cryptography

How Are Keys Generated?

- Generate a large random number (can be based on multiple random numbers to "assure" randomness)
- Use the random number for a key generating function to generate a pair of keys
- The random number is discarded, thus nobody could regenerate the pair

Reference, a RSA key generation algorithm:
http://en.wikipedia.org/wiki/RSA

Public Key Cryptography

How To Bind a Public Key to Its User?

- Public-key infrastructure (PKI)
  - » To provide trusted third party (Certifying Authority) to use identity certificates to bind public keys to users
  - » May refer to the software that manages certificates in a large-scale setting

- A certificate may be revoked – to check the certificate revocation list (CRL)

Public Key Cryptography

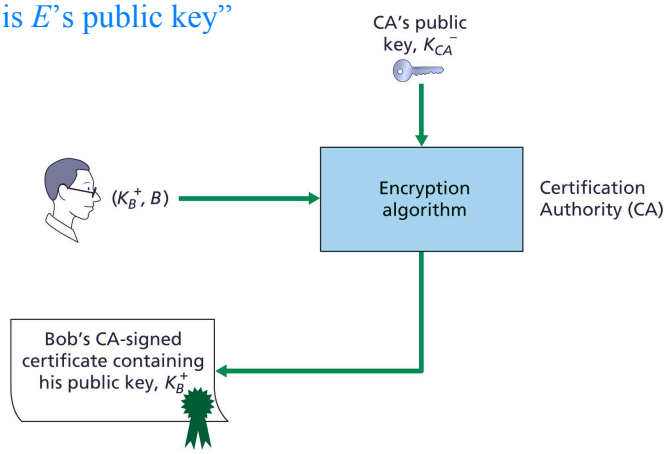
How to Generate a Certificate?

- Generate a public-private key pair from a large random number
- Keep the private key, send the public key and identifying information to a Certificate Authority (CA)
- Pay a fee to the CA
- The CA verifies the identity
- The CA creates a certificate (including all ID information and the URL of the web site home)
- The CA *signs* the certificate (encoded with its own private key) and sends the signed certificate to you

Key Distribution and Certification

Certification Authorities

- 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"

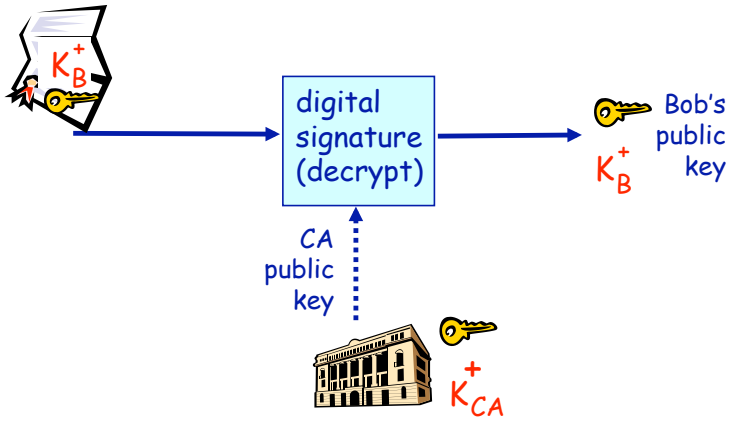


Key Distribution and Certification
Certification Authorities

When Alice wants Bob's public key:

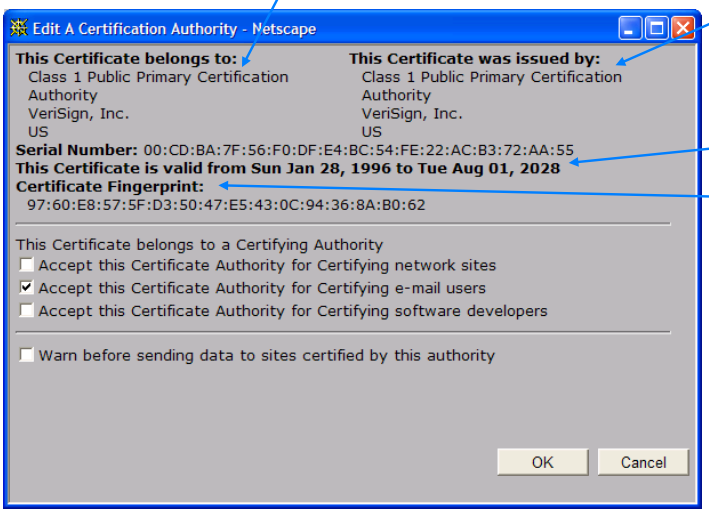
» get Bob's certificate (Bob or elsewhere).

» apply CA's public key to Bob's certificate, get Bob's public key



Key Distribution and Certification
Example Certificate

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



- Info about certificate issuer
- Valid dates
- Digital signature by issuer

Using Public Key Cryptography

- A key generation algorithm
  - » For generating a public key with its paired private key
- A signing algorithm
  - » Using private key to encrypt sender's description into digital signature
- A verification algorithm
  - » Using sender's public key to decode and match sender's digital signature

Authentication

- Certificate Authorities (CAs)
  - » Issue digital certificates
  - » Many commercial CAs, e.g. VeriSign
  - » Is an example of a trusted third party
- Web browsers and other encryption software are delivered with the signed certificates of a number of well known CAs, called root CAs.
- A server obtains a digital certificate from a CA, who verifies the certificate recipient

Client's Action in Authentication

- Check the validity of the certificate
  - » Certification revocation list
- Decrypt the sender encrypted signature with the provided public key
- Compare description on the unencrypted information with the decrypted signature, authenticated if match
- The public key is used by client for later encryption to the server and decryption from the server

SSL (Secure Socket Layer) and TLS (Transport Layer Security)

- These protocols implement security described above over the Internet
- Run below application protocols (HTTP, SMTP, et.) and above TCP transport protocol

References:
http://en.wikipedia.org/wiki/Secure_Sockets_Layer
http://www.verisign.com/products-services/security-services/ssl/

SSL and TLS

- SSL by Netscape
- TLS, successor of SSL
  - » an IETF (International Engineering Task Force) standard protocol
- Provide, over the Internet
  - » Endpoint authentication
    - ❖ typically, the server is authenticated, but not the client
  - » Communications privacy
    - ❖ asymmetric cryptography

HTTPS servers

- Apache-SSL
  - » Separate from the Apache project, due to government export restrictions
  - » Available in the US, via: http://www.apache-ssl.org/
  - » Free for all
  - » 128 bit encryption worldwide

What Careful Users Should Do

- To be "sure" of secure communication
  - » For financial or other crucial applications, deal only with https servers, i.e. URL with https:// protocol
  - » When receiving a warning about wrong certificate
    - It could bear a name similar to the intended server.
    - Your request may have been intercepted by a fake server.
    - Continued communication may cause you trouble.
    - What you should do
      - Cancel current request
      - Resubmit request
      - Continue only if no more warning is received

What Careful Users Should Do

- Remember that security may still be violated at the server site
  - » Sever site could be broken into
  - » Human problems at server site