Digital Signatures

Digital Signatures

- Offer similar protections as hand-written signatures in the real world.
  1. Difficult to forge.
  2. Easily verifiable.
  3. Not deniable.
  4. Easy to implement.
  5. Differs from document to document.

Message Hash

- A message hash is a checksum like value or condensed version of a file.
- Any change to a file will produce a different message hash.
- Message hashes are one way functions. There is no known method of creating a data file to match a known message hash.
- SHA-1 is a Standard Hash Algorithm
- SHA-1 creates a 160 bit hash value

Message Authentication Codes

- A message authentication code (MAC) verifies that the message has not been modified by anyone who does not know the key
- MAC is created by encrypting a message hash.
- Any encryption algorithm can be used.

MAC Use

- When creating the file
  - compute the hash
  - encrypt the hash
  - append the hash to the file
- When reading the file
  - compute the hash
  - encrypt your hash
  - compare your hash to the one in the file

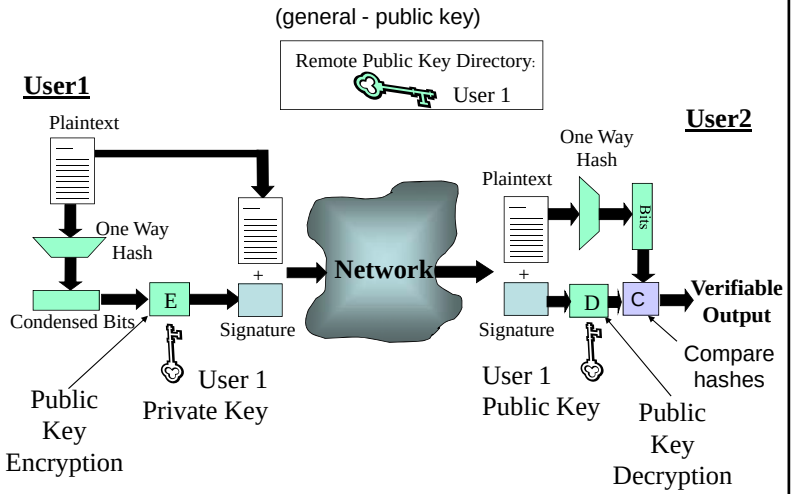
Digital Signature

- Digitally signed messages can have clearly viewed plaintext in the body of the message, the objective is to verify the sender.
- With RSA public key encryption either key can be used to encrypt or decrypt.

Digital Signature Process

- A hash of the data is created. The name of the sender is appended to the hash.
- The hash is encrypted with the private key of the sender.
- The hash is appended to the data and transmitted together.
- The receiver decrypts the hash with the public key of the sender.
- The receiver calculates a hash of the message and compares it to the received hash.

Digital Signature



Digital Signature Use

- Digitally signed email verifies the sender.
- Signed applets or programs come from a known source and have not been modified.
- Digitally signed programs cannot be modified or infected with a virus without detection
- Digitally signed documents cannot be changed without detection.

Key Distribution

- If you are going to rely on public key encryption, it is necessary to ensure the authenticity of public keys.
- Keys can be distributed by
  - Key Servers
  - Digital Certificates

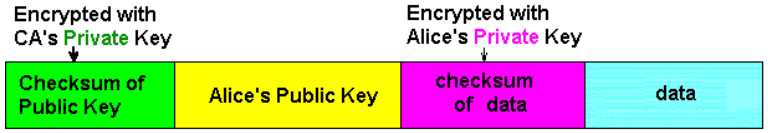
Key Servers

- Key servers are computers that have a database of public keys.
- Upon receiving a request for a public key, a key server sends the client the desired public key.
- The messages from the key server are digitally signed.
- Clients have to know the key server's public key.

Digital Certificates

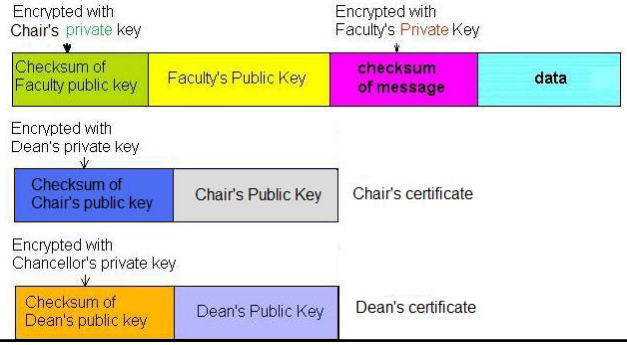
- A digital certificate contains a user's public key along with some information about the user, such as their email address.
- The digital certificate is digitally signed by a Certificate Authority.
- Certificate Authorities are venders of digital certificates.
- Clients must know the public key of the Certificate Authority.

Digital Certificates



University Certificates

- A chain of trust can be established from a single point in an organization.
- Only the top public key is needed by everyone



Buying Digital Certificates

- Several companies sell digital certificates
- They are usually expensive

Creating Digital Certificates

- Security tools available with Java SDK

Tool Name	Brief Description
keytool	Manage keystores and certificates.
jarsigner	Generate and verify JAR signatures
policytool	GUI tool for managing policy files.

Security Tool Documentation

- The security tools are command line programs with many options

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/jarsigner.html

KeyStore

- The Java key tools use a keystore as a place to securely keep
  - key entries
  - trusted certificate entries
- A keystore can be encrypted for security
- Implemented as a file containing the information

Signing Assignment

- Create a digital certificate containing your name
- Digitally sign a jar file containing your steganography program
- Send it to me by Wednesday, January 27