Security

Levels of Threat

The level of system security required depends upon the expertise of the attacker.

1. Ordinary web user
2. Sophisticated user *(CS students)*
3. Professional Thief
4. Insider
5. Corporate
6. Government

Cost of Security

- Security has a cost in hardware, software and user convenience.
- The cost of defeating a security system must be greater than the value of the data it protects.

Security Goals

The goals for protecting any system are to assure that the following criteria are met:

1. **Integrity Control**– data is created/modified by authorized parties only.
2. **Secrecy/Confidentiality** – access is restricted to authorized parties.
3. **Authentication** – verifying identity
4. **Non-repudiation** – verification of action or data
5. **Availability** – services up and running.

Threats to System Security

Threats to network security typically come in any of four forms:

1. **Interception** – sniffing, wiretapping, eavesdropping
2. **Modification** – unauthorized access/tampering
3. **Fabrication** – impersonation or fabrication of data or objects to gain access to services/information.
4. **Interruption** – Denial of Service

Methods of Attack

- Eavesdropping
  - Viewing data or passwords on the network.
  - Easy to do on broadcast networks.
- Message Tampering
  - Changing messages as they travel the network.
- Masquerading
  - Sending messages and programs with invalid sender identification.

Methods of Attack (cont.)

- Replay
  - Interception and duplication of transmissions at a later time.
- Denial of Service
  - Crashing the system or flooding it with messages or tasks.
- False Identification
  - Password Guessing
- Malicious Software
  - Viruses, Worms, Trojan Horses, etc.

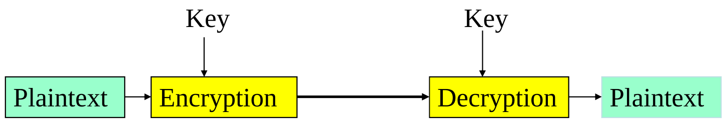
Methods of Defense

- Cryptography – encoding of data or messages
- Software Controls – Antivirus
- Hardware Controls – smartcards, biometrics
- Physical Controls – locked doors
- Security Policies & Procedures
- User Education
- Penalty of Law

- for effective security, many/all of the above should be utilized in cooperation/coordination.

Cryptography

- Cryptography in general represents the process of encrypting a plain-text file into an unreadable cipher so that it can be stored and decrypted by the intended recipient.
- Cryptography is an important tool for security.



Key

Key

Plaintext

Encryption

Decryption

Plaintext

Encryption Media

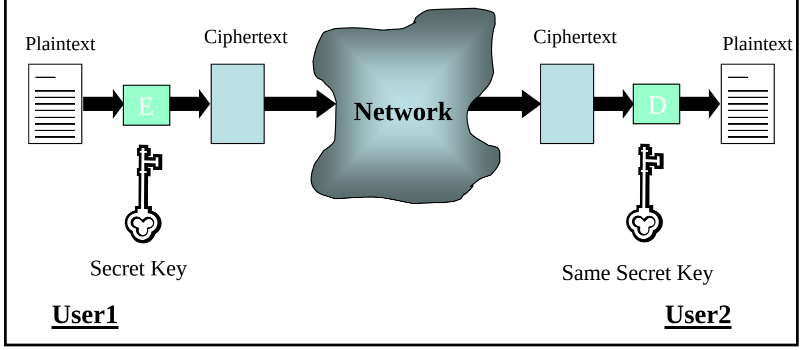
- Encryption can be used to secure messages sent over a network.
- Encryption can also be used to secure data stored on a computer.
- Think of a data file as a very slow message.

Types of Encryption

- Secret Key
  - The encryption key is the same as the decryption key.
  - Sender and receiver have to securely share a key.
- Public Key
  - The key to decrypt is different, but related to, the key to encrypt.
  - The encryption key can be made public while the decryption key is kept secret.

Secret Key Cryptography

- Keys exchanged prior to communications. Parties verified at that time.
- Key to encrypt message is the same as key to decrypt.
- DES and AES encryption are examples of Secret Key Cryptography.



Plaintext

Ciphertext

Network

Ciphertext

Plaintext

E

D

Secret Key

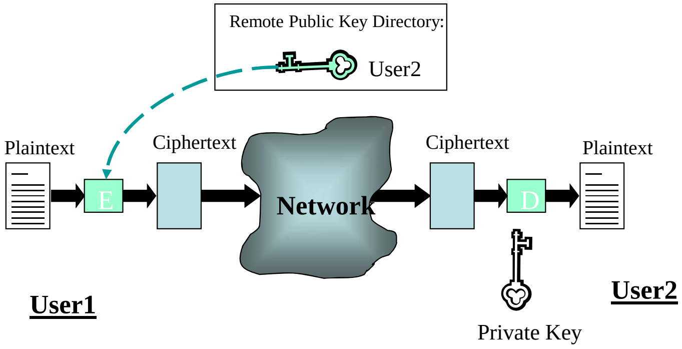
Same Secret Key

User1

User2

Public Key Cryptography

- Public key different from private key.
- RSA and Elliptic Curve Cryptography (ECC) encryption are examples of Public Key Cryptography.



Encryption Performance

- RSA Public key encryption is slower than DES or AES.
- DES and AES are easy to implement in hardware.
- AES can be efficiently implemented in software.
- Hybrid encryption uses both public and secret key systems.

Key Strength

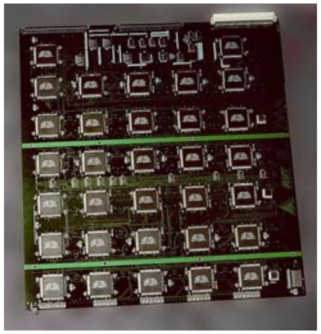
- The longer they key, the harder it is to defeat the encryption by brute force.
- If the key is n bits, it requires 2^n guesses to try all possible keys. You are likely to guess correctly in 2^{n-1} tries.
- Public key algorithms require a mathematical relation between the keys so not every bit string can be a key.

Key Lengths

- DES uses a 56 bit key
- Triple DES or DES3 uses two DES keys for a total of 112 bits
- AES uses 128, 192 or 256 bit keys.
- RSA uses variable length keys, frequently 512, 1024 or 2K bits in length.

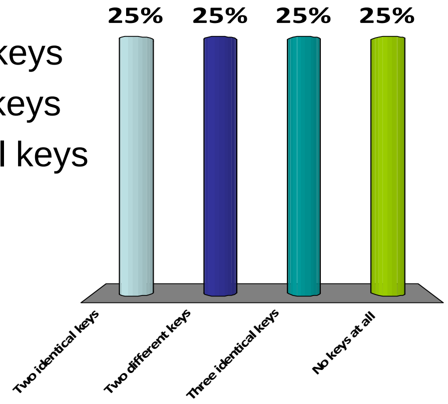
Brute Force Decryption

- Brute force tries all possible keys.
- In 1998 the Electronic Frontier Foundation built a device that could brute-force a DES key in a little more than 2 days



Public key encryption uses

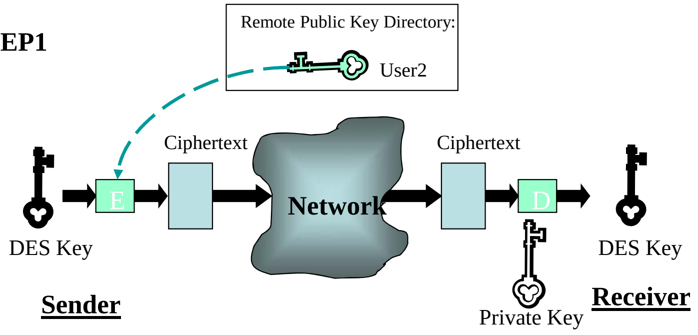
1. Two identical keys
2. Two different keys
3. Three identical keys
4. No keys at all



Hybrid Cryptography (STEP 1)

- DES key is encrypted with public key cryptography using Public Key of receiver.
- DES key sent to receiver.
- Both users end up with a shared DES key.

STEP1



Remote Public Key Directory:

User2

Ciphertext

Ciphertext

E

Network

D

DES Key

DES Key

Private Key

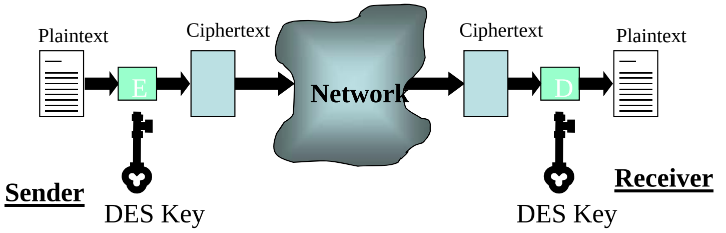
Sender

Receiver

Hybrid Cryptography (STEP 2)

- Message is encrypted with the DES key previously sent to the receiver.
- DES key is discarded after sending the message.

STEP2



Plaintext

Ciphertext

Ciphertext

Plaintext

E

Network

D

Sender

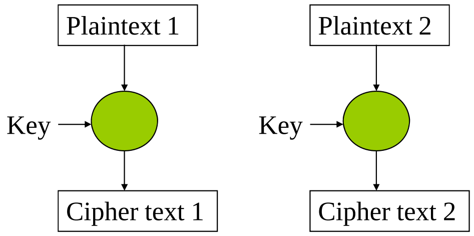
DES Key

Receiver

DES Key

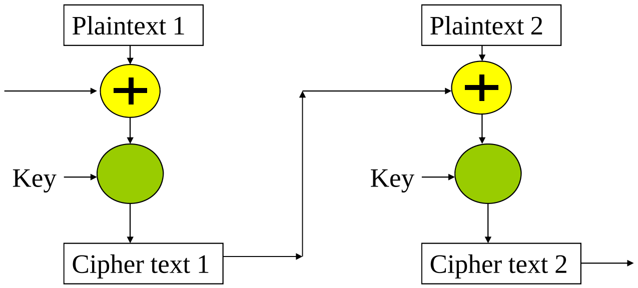
Encryption Methods

- Block Cipher – one block of plaintext is encrypted to one block of cipher text.



Encryption Methods

- Stream Cipher – blocks are XORed with previous blocks.



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

Digital Signature

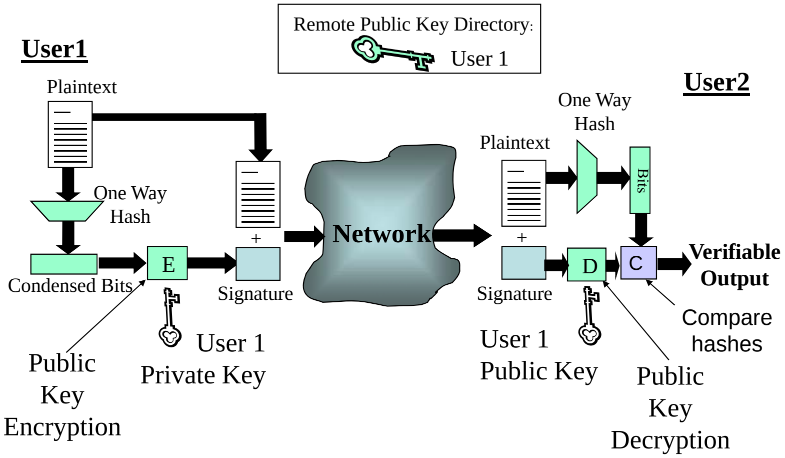
- Digitally signed messages can have clearly viewed plaintext in the body of the message, the objective is to verify the sender.
- With RSA public key encryption either key can be used to encrypt or decrypt.

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.

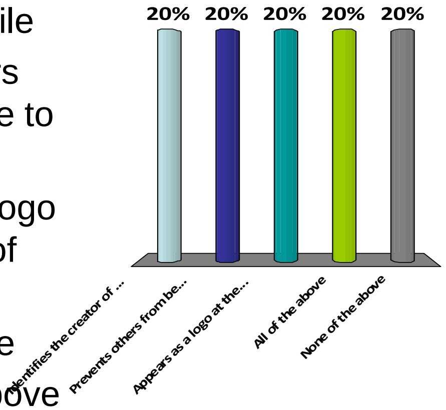
Digital Signature

(general - public key)



A digital signature

1. Identifies the creator of the file
2. Prevents others from being able to read the file.
3. Appears as a logo at the bottom of the file.
4. All of the above
5. None of the above



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.
- Digitally signed documents cannot be changed.

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

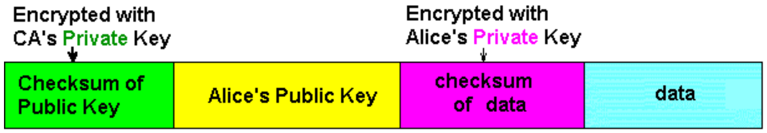
Key Servers

- 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



Encrypted with CA's Private Key

Encrypted with Alice's Private Key

Checksum of Public Key

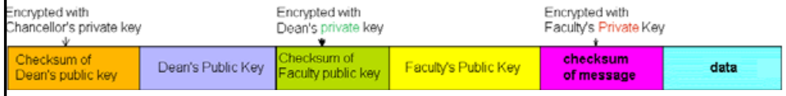
Alice's Public Key

checksum of data

data

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



Encrypted with Chancellor's private key

Encrypted with Dean's private key

Encrypted with Faculty's Private Key

Checksum of Dean's public key

Dean's Public Key

Checksum of Faculty public key

Faculty's Public Key

checksum of message

data

Secure Sockets Layer (SSL)

- SSL is a popular form of secure communications that is widely used within commercial applications.
- Combines elements of public and private key encryption and digital signature.
- Used by HTTPS

Actions of SSL

1. Authenticates the server to the client.
2. Allows the server and client to select the cryptographic algorithms they support.
3. Optionally authenticate client to server.
4. Use public key encryption to generate shared secrets.
5. Establish an encrypted SSL connection.

Firewalls

- Firewalls filter information that passes from the outside world into a private network.
- Firewalls can be implemented in a router.
- A firewall can restrict certain types of traffic activity on a network based on:
  - Source or destination IP address
  - Port number
  - Protocol
  - data contents (virus scanning)

Authentication

- How do you know the user is who they claim to be?
- Typically authenticated by something you:
  - know
  - have
  - are
  - can do

Biometrics

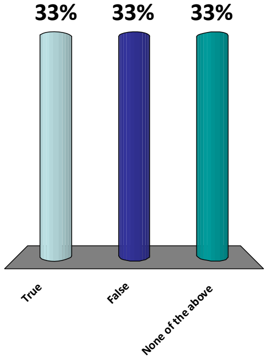
- Biometrics is the measuring of some physical or biological property of a person.
- Examples include fingerprints readers and retinal eye scanners.
- While you can change your password, you cannot change your biometrics.
- If somebody else measures your biometrics, it may be possible to masquerade as you.

Login Authentication

- Most systems request a userid and password to login.
- Sending the password in clear text is not secure.

Sending the password encrypted provides secure authentication

1. True
2. False
3. None of the above



Secure Authentication

- If the server and the client share an encryption key

Client	**Server**
Send ID & nounce1	
	Send encrypted nounce1& nounce2
Send encrypted nounce2	
	Send OK

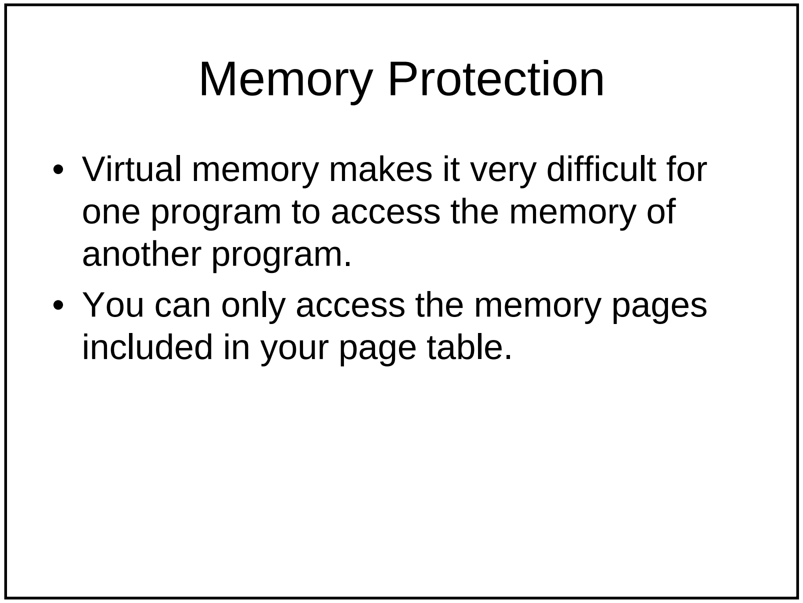
Malicious Software Zoo

- **Trojan Horse** – Functionality hidden in a software package.
- **Worm** – Self replicating software
- **Virus** – Self replicating software that attaches itself to other programs.

- Malicious software can only attack a system if it is executed.

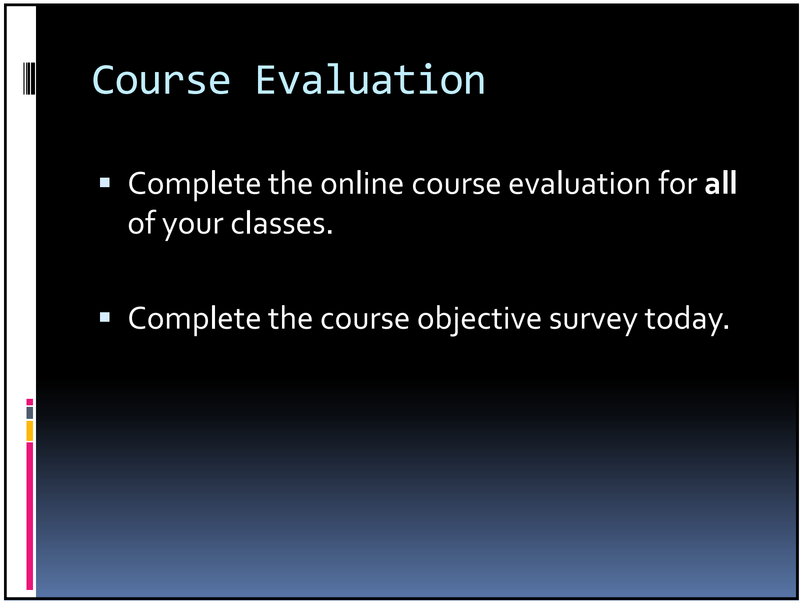
Pentium Protection

- Protection bits give 4 levels of privilege
  - 0 most protected, 3 least
  - Use of levels is software dependent
  - Usually level 3 for applications, level 1 for O/S and level 0 for kernel (level 2 not used)
  - Level 2 may be used for apps that have internal security e.g. database
  - Some instructions only work in level 0



Memory Protection

- Virtual memory makes it very difficult for one program to access the memory of another program.
- You can only access the memory pages included in your page table.



Course Evaluation

- Complete the online course evaluation for **all** of your classes.
- Complete the course objective survey today.