# Networks & Server Structures

Cryptography

Digital Certificates

RAID

Consumer Configurations

# Cryptography

01000101 01110100 00100000 01101001 01101110 00100000 01000001 01110010 01100011 01100001 01100100 01101001 01100001 00100000 01000101 01100111 01101111

# Cryptography

- The process of converting readable text (plaintext) into an unreadable series of characters and symbols (cipher-text)
- Allows you to transmit sensitive information over unsecured networks (such as the Internet)
- Keys are secret values used to encrypt and decrypt messages

# Cryptography

- 3 Primary Functions
  - Confidentiality
  - Authentication
  - Integrity

# Keys

- A piece of information that determines the functional output of a cryptographic algorithm or cipher.
- Secret values used to encrypt and decrypt messages
- Without a key, the algorithm would produce no useful result

# Encryption Methods

- Symmetric
- Asymmetric

# Symmetric Encryption

- Encryption key can be calculated from the decryption key and vice versa
- In most cases the encryption and decryption keys are the same
- Require the sender and receiver to agree on a key before they communicate securely
- Problem with transmitting the key(s)

# Asymmetric Encryption

- **Public Key Cryptography**
- Encryption and decryption key are different
- Decryption key cannot be calculated from the encryption key
- Allows a host's encryption key to be made public (public key)
- Decryption key must be kept secret (private key)
- Much slower than symmetric encryption

# Key Exchange

- Bob puts symmetric key in box, locks it with his secret key & sends to Sue
- Sue places her lock on the box and locks it with her secret key.  Sends back to Bob
- Bob removes his lock & sends back to Sue
- Sue removes her lock and can now open the box

# Hashing

- Takes a variable length input and converts it into a fixed length output string (called a hash value)
- Used to verify that the data received is the same as the data that is sent
- One way.  Cannot undo a hash.
- Used in digital certificates and for encrypting stored passwords

# Hashing

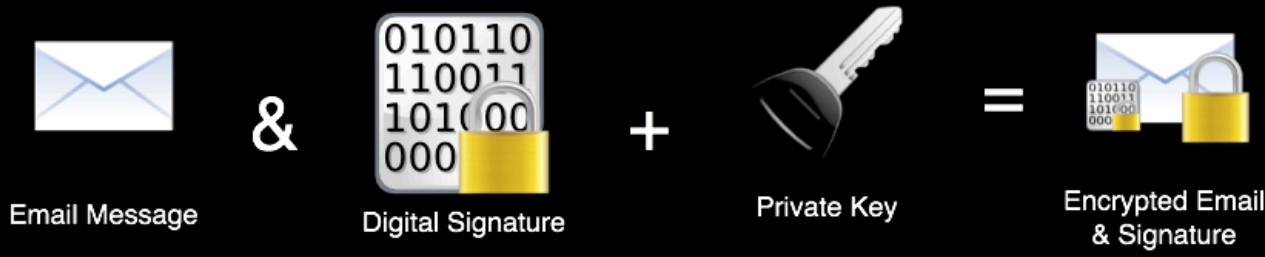
- 2 most common
- SHA-1 (Secure Hash Algorithm 1)
- Developed by the NSA
- MD5 (Message Digest algorithm version 5)
- Developed by RSA

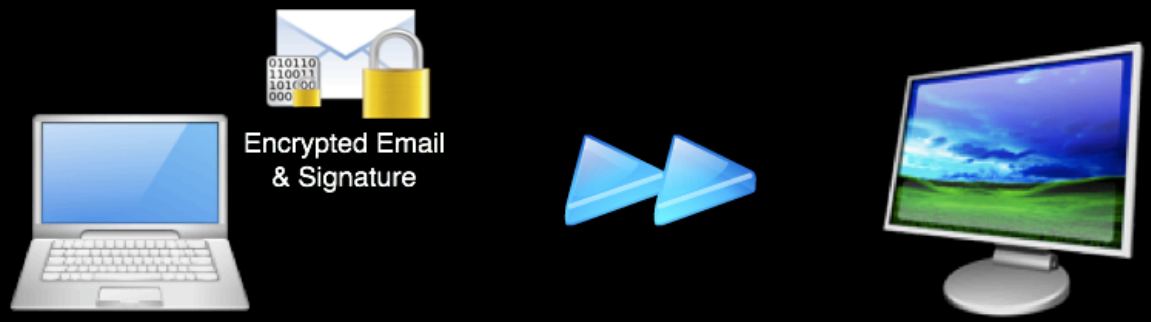
# Digital Signature

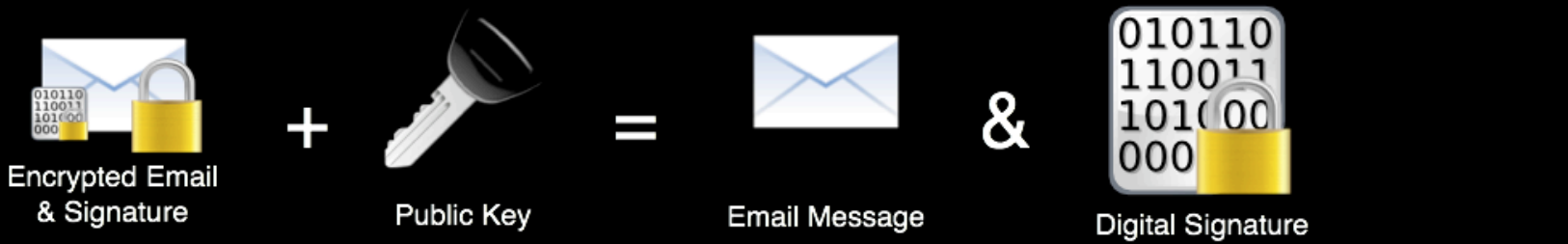
- If a public key can successfully decrypt a message, then the only person who could have performed the encryption is the holder of the corresponding private key
- Perform a hash on the message, then encrypt the message digest using your private key
- Recipient hashes the message using the same algorithm then decrypts the signature using the public key


Email Message
Hash Function
Message Digest


Message Digest
Private Key
Digital Signature

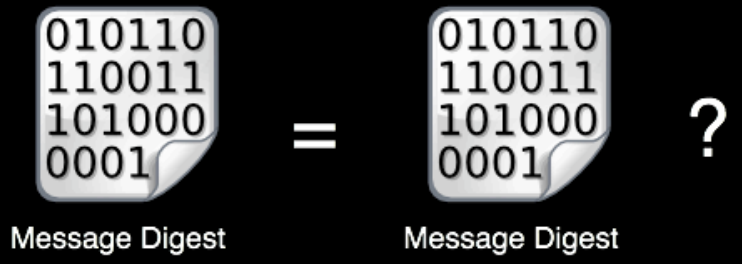

Email Message
Digital Signature
Private Key
Encrypted Email & Signature


Encrypted Email & Signature


Encrypted Email & Signature
+
Public Key
=
Email Message
&
Digital Signature


Email Message
+
Hash Function
=
Message Digest


Digital Signature
+
Public Key
=
Message Digest


Message Digest
=
Message Digest
?

# Create a Public Key

Will be used for authentication to the Web Dept server

1. Open Terminal
2. cd ~
3. ls -la
4. cd .ssh
5. ls -l

# Create a Public Key

6. ssh-keygen -t rsa -N “” -f id_rsa
7. ls -l
8. scp id_rsa.pub user@66.192.104.111:~/
9. ssh user@66.192.104.111
10. ls -la
11. mkdir .ssh

# Create a Public Key

12. cat id_rsa.pub >> .ssh/authorized_keys
13. exit
12. ssh user@66.192.104.111

# Digital Certificate

- Used to verify that the person sending the information is really who they say they are
- Issued by a certificate authority - a private company that charges users or companies for the issuance of the certificates

# Firewalls

- Access Control List (ACL)
- A system that enforces a security policy between two networks
- Software or Hardware device that inspects traffic coming through it and either permits or denies it based on a set of rules


# RAID

...wrong

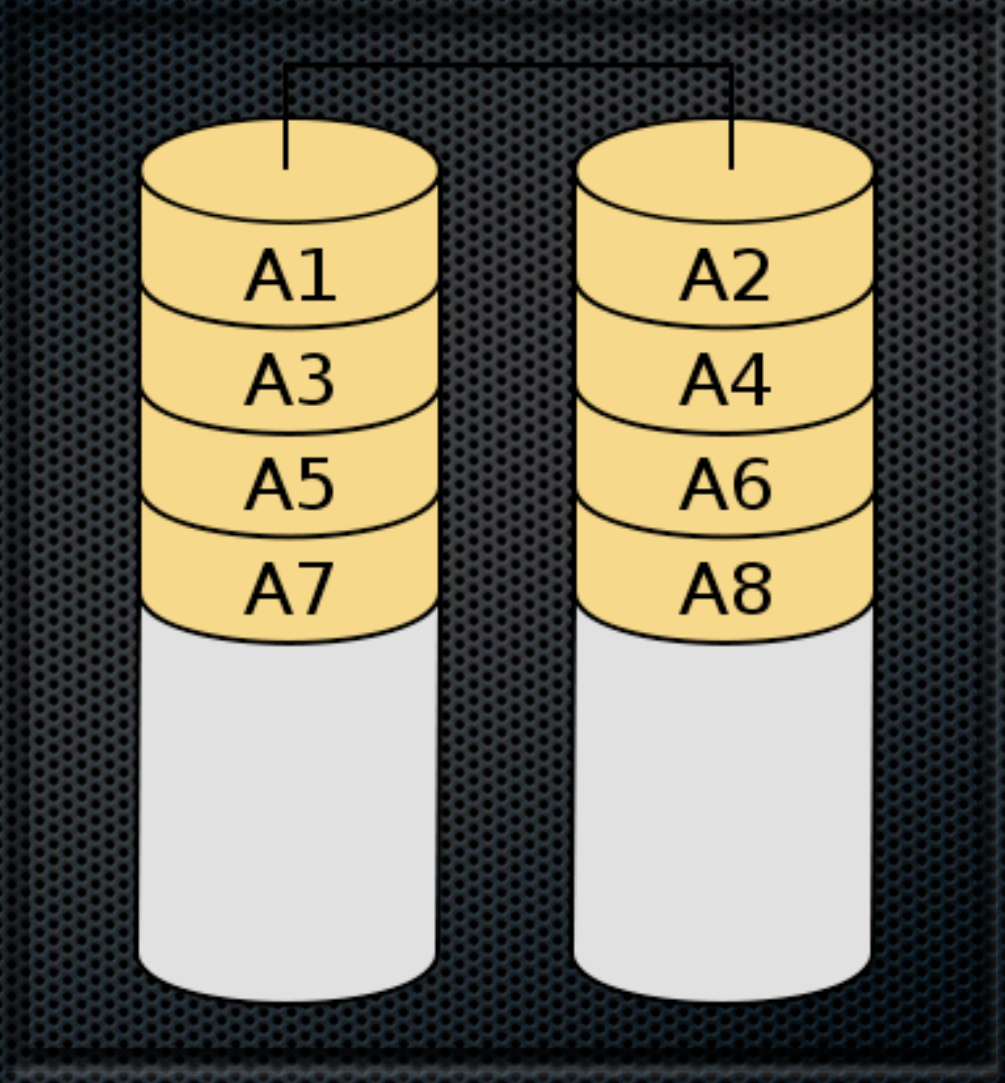
# R.A.I.D.

- Redundant Array of Independent Disks
- Uses multiple hard disk drives simultaneously to improve performance or reliability

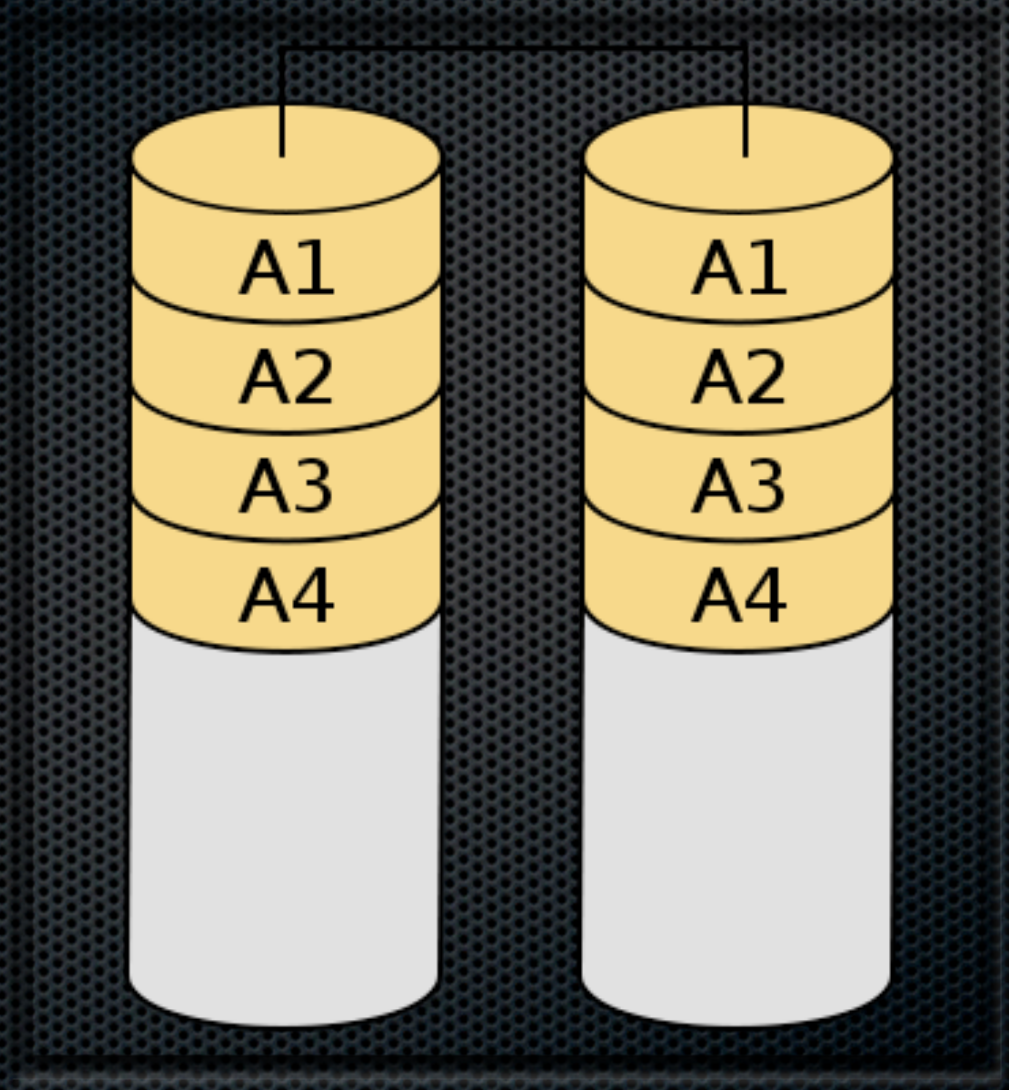
# R.A.I.D.

- RAID 0 - Striped
  - Sets multiple disks up as a single drive
  - Can improve speed
- RAID 1 - Mirrored
  - Stores the same data on each disk
  - Fault tolerant
- RAID 5 - Striping with Parity
  - 3 or more disks used
    - Fault tolerant

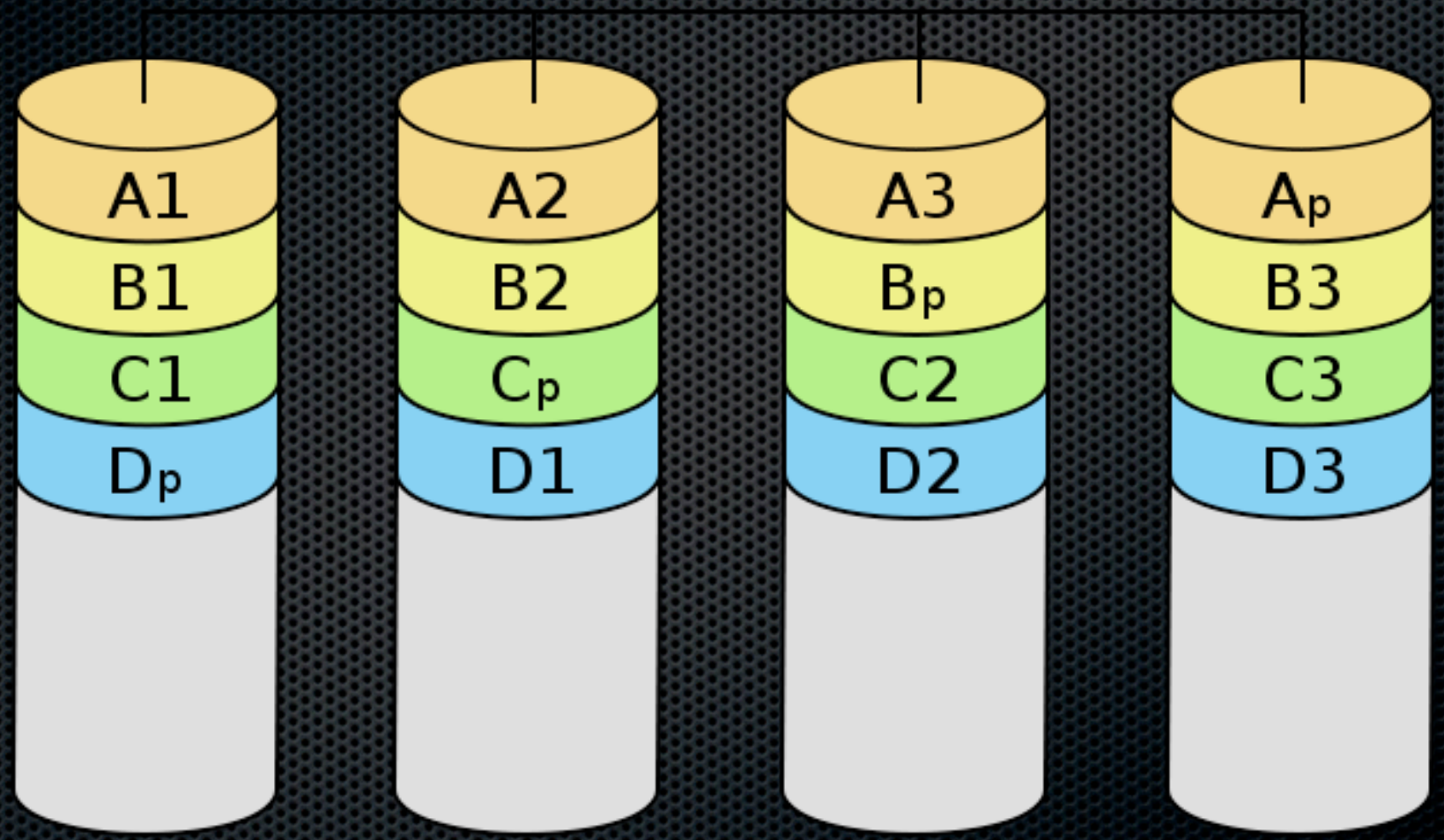
# RAID 0



# RAID 1



# RAID 5



# HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three maior online businesses are ——

**. . . & blow your family to smithereens!**

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

# Protecting Yourself Online

..because hackers can blow you up

# Protecting Yourself

- Use strong passwords
- Use a NAT router at home (creates a hardware firewall)
- Use a software firewall on your computer when you are not at your home network
- Do not open attachments in emails
- Do not follow links in emails that take you to log in pages

# Protecting Yourself

- Do not log into anything important while on a public WiFi
  - Consider using a VPN
- Do not log into anything without making sure your connection is encrypted
- Have antivirus and anti-spyware software installed and keep it up to date
- Be careful when downloading software
- Pay attention to cookies

# Protecting Yourself

- Think twice about disclosing any personal information.
- Avoid using your real name online.
- Be especially cautious of ‘friends’ who you have just met online but who ask you to reveal personal information or want to meet you offline.
- Be wary of disclosing personal information on a work or personal web site.
- Use a disposable, anonymous email account for websites that demand an email address to register.

# Protecting Yourself

- Java, Javascript and ActiveX can do horrible things to you
- Keep your OS patches up to date
- Keep your software updated
- Don’t run as administrator or root for regular day to day tasks

# Backup Your Data

- Keep regular backups of important data (documents, photos, music, etc)
- Backup locally and off site
  - Carbonite
  - Mozy
  - Backblaze
- Unverified backups are not backups

# Hoaxes

- Usually just a nuisance but can be used by spammers to collect email addresses or do worse things
- Bogus virus warnings
- The promise of free gifts or cash for forwarding an email
- Chain letters (“forward this to ten people for good luck”)
- Pyramid schemes that promise a massive payback if you forward the message to enough people
- Bogus email asking for a donation to a disaster fund
- Emails that maliciously target individuals and make trouble for them.

# Wireless Network Encryption

- WEP - Wired Equivalent Privacy
- WPA - WiFi Protected Access
- Not protocols or encryption but certification from the Wi-Fi Alliance

# WPA

- **WPA PSK** - Pre Shared Key
  - All devices use the same key
  - Can cross decrypt each other's traffic
  - Not good for corporate environment
- **WPA TKIP** - Temporal Key Integrity Protocol
  - Still uses RC4 like WEP but *tried* to fix the problems
- **WPA AES** - Advanced Encryption Standard

# WPA vs WPA2

- Remember WPA is just a certification.  So WPA2 is just a different level of certification.  The underlying cyphers and protocols are the same.
- Based on what equipment you are using