COURSE TECHNOLOGY
CENGAGE Learning™

# Cryptography

*CISSP Guide to Security Essentials*

*Chapter 5*

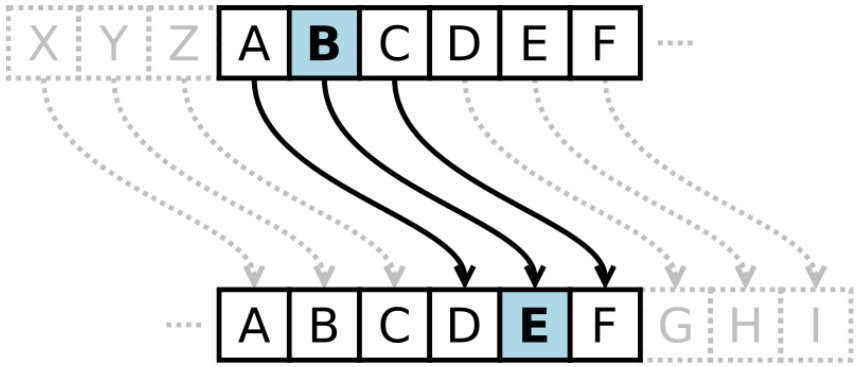
# Objectives

- Applications and uses of cryptography
- Encryption methodologies
- Cryptanalysis
- Management of cryptography
- Key management

# Applications and Uses of Cryptography

# What Is Cryptography

- Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized parties.
  - Substitution cipher first used by Caesar for battlefield communications



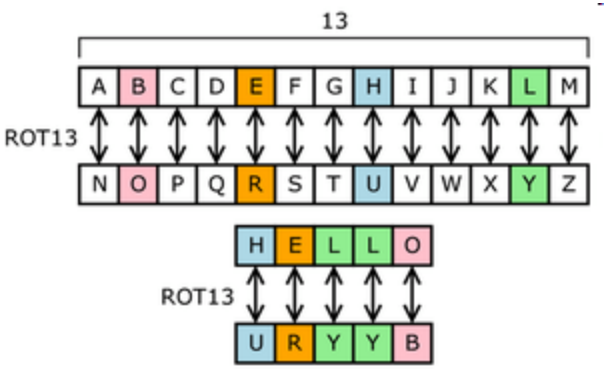
# Encryption Terms and Operations

- Plaintext – an original message
- Ciphertext – an encrypted message
- Encryption – the process of transforming plaintext into ciphertext (also *encipher*)
- Decryption – the process of transforming ciphertext into plaintext (also *decipher*)
- Encryption key – the text value required to encrypt and decrypt data

# Encryption methodologies

# Substitution Cipher

- Plaintext characters are substituted to form ciphertext
  - “A” becomes “R”, “B” becomes “G”, etc.
  - Character rotation
    - Caesar rotated three to the right (A > D, B > E, C > F, etc.)
  - A table or formula is used
  - ROT13 is a Caesar cipher
  - Image from Wikipedia (link Ch 5a)
  - Subject to *frequency analysis* attack



# Transposition Cipher

- Plaintext messages are transposed into ciphertext

| | | | | |
|---|---|---|---|---|
| **A** | **K** | **C** | **N** | **B** |
| **T** | **A** | **E** | **O** | **R** |
| **T** | **T** | **V** | **R** | **I** |
| **A** | **O** | **I** | **T** | **D** |
| **C** | **N** | **A** | **H** | **G** |

Plaintext:

ATTACK AT ONCE VIA
NORTH BRIDGE

  - Write into columns going down
  - Read from columns to the right

# Transposition Cipher (cont.)

Ciphertext:

AKCNBTAEORTTVRIAOITDCNAHG

- Subject to *frequency analysis* attack

| | | | | |
|---|---|---|---|---|
| **A** | **K** | **C** | **N** | **B** |
| **T** | **A** | **E** | **O** | **R** |
| **T** | **T** | **V** | **R** | **I** |
| **A** | **O** | **I** | **T** | **D** |
| **C** | **N** | **A** | **H** | **G** |

# Monoalphabetic Cipher

- One alphabetic character is substituted or another
  - Caesar right-three shift:

| A | B | C | D | E | F | G | H | I | J | … | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| D | E | F | G | H | I | J | K | L | M | … | C |

  - Or a more random scheme:

| A | B | C | D | E | F | G | H | I | J | … | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| W | E | R | T | B | N | P | Q | C | U | … | X |

- Subject to *frequency analysis* attack

# Polyalphabetic Cipher

- Two or more substitution alphabets

| Plaintext | A | B | C | D | E | F | G | H | I | … | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Alpha 1 | W | E | R | T | B | N | P | Q | C | … | X |
| Alpha 2 | R | B | I | K | Q | D | X | U | N | … | E |
| Alpha 3 | V | B | D | R | H | W | A | X | I | … | U |
| Alpha 4 | M | U | T | X | D | G | P | O | W | … | F |
| Alpha 5 | Y | D | V | B | J | I | K | E | Z | … | O |

# Polyalphabetic Cipher (cont.)

| Plaintext | A | B | C | D | E | F | G | H | I | … | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Alpha 1 | W | E | R | T | B | N | P | Q | C | … | X |
| Alpha 2 | R | B | I | K | Q | D | X | U | N | … | E |
| Alpha 3 | V | B | D | R | H | W | A | X | I | … | U |
| Alpha 4 | M | U | T | X | D | G | P | O | W | … | F |
| Alpha 5 | Y | D | V | B | J | I | K | E | Z | … | O |

- CAGED becomes  RRADB
- Not subject to *frequency attack*

# Running-key Cipher

- Plaintext letters converted to numeric (A=0, B=1, etc.)
- Plaintext values “added” to key values giving ciphertext

# Running-key Cipher

- Modulo arithmetic is used to keep results in range 0-26
  - Add 26 if results < 0; subtract 26 if results > 26

| Plaintext | A | T | T | A | C | K | A | T | O | N | C | E | V | I | A | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | S | E | C | R | E | T | S | E | C | R | E | T | S | E | C | R |
| Plaintext | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 14 | 13 | 2 | 4 | 21 | 8 | 0 | 13 |
| Key | 18 | 4 | 2 | 17 | 4 | 19 | 18 | 4 | 2 | 17 | 4 | 19 | 18 | 4 | 2 | 17 |
| Sum | 18 | 23 | 21 | 17 | 6 | 3 | 18 | 23 | 16 | 4 | 7 | 23 | 11 | 12 | 2 | 4 |
| Ciphertext | S | X | V | R | G | D | S | X | Q | E | H | X | L | M | C | E |

# One-time Pad

- Works like running key cipher, except that key is length of plaintext, and is used only once
- Highly resistant to cryptanalysis

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext | A | T | T | A | C | K | A | T | O | N | C | E | V | I | A | N |
| Key | X | V | G | J | E | R | I | O | Q | W | J | P | E | K | A | F |
| Plaintext | 0 | 19 | 19 | 0 | 2 | 10 | 0 | 19 | 14 | 13 | 2 | 4 | 21 | 8 | 0 | 13 |
| Key | 23 | 21 | 6 | 9 | 3 | 17 | 8 | 14 | 16 | 22 | 9 | 15 | 4 | 10 | 0 | 5 |
| Sum | 23 | 14 | 25 | 9 | 5 | 1 | 8 | 7 | 4 | 9 | 11 | 19 | 25 | 18 | 0 | 18 |
| Ciphertext | X | O | Z | J | F | B | I | H | E | J | L | T | Z | U | A | U |

# Types of Encryption

- Block cipher
  - Encrypts blocks of data, often 128 bits
- Stream cipher
  - Operates on a continuous stream of data

# Block Ciphers

- Encrypt and decrypt a block of data at a time
  - Typically 128 bits
- Typical uses for block ciphers
  - Files, e-mail messages, text communications, web
- Well known encryption algorithms
  - DES, 3DES, AES, CAST,  Twofish, Blowfish, Serpent

# Block Cipher Modes of Operation

- Electronic Code Book (ECB)
- Cipher-block chaining (CBC)
- Cipher feedback (CFB)
- Output feedback (OFB)
- Counter (CTR)

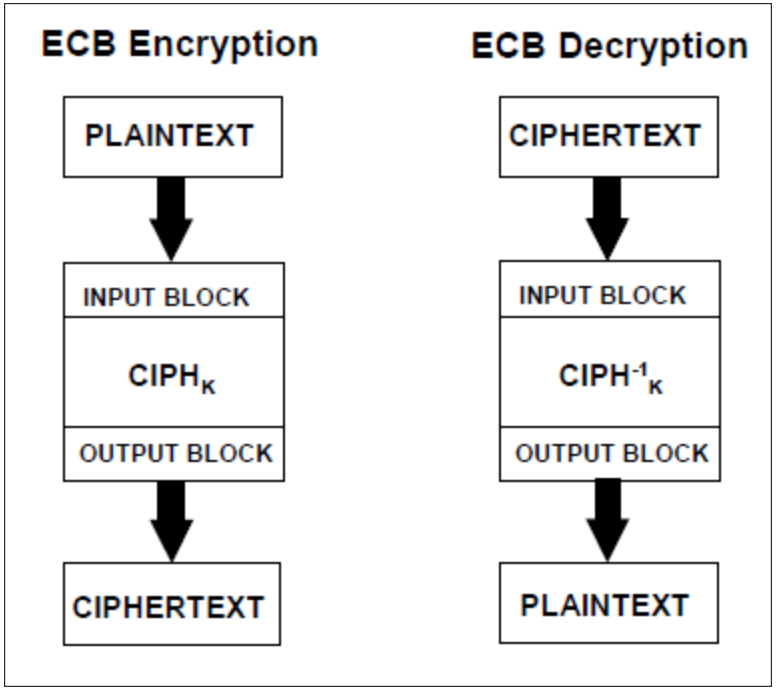
# Initialization Vector (IV)

- Starting block of information needed to encrypt the first block of data
- IV must be random and should not be re-used
  - WEP wireless encryption is weak because it re-uses the IV, in addition to making other errors

# Block Cipher: Electronic Code Book

- Simplest block cipher mode
- Each block encrypted separately
  - Like plaintext encrypts to like ciphertext
  - Vulnerable to a *dictionary attack*
  - WEP does this
  - Microsoft made this error in their password hashes
  - Microsoft also made this error in Microsoft Office document encryption

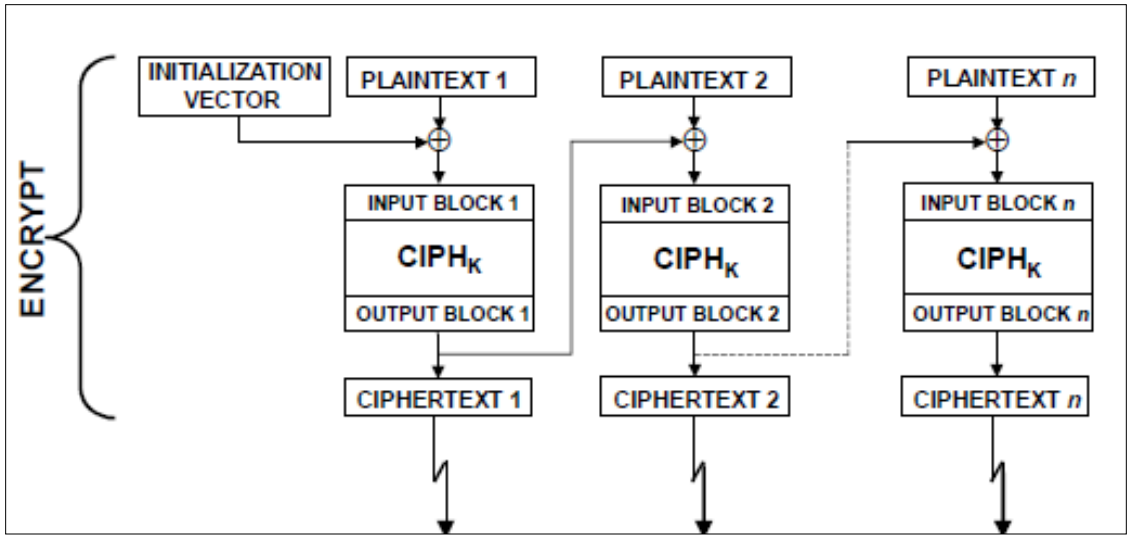
# ECB Mode




- Images from NIST (link Ch 5d)

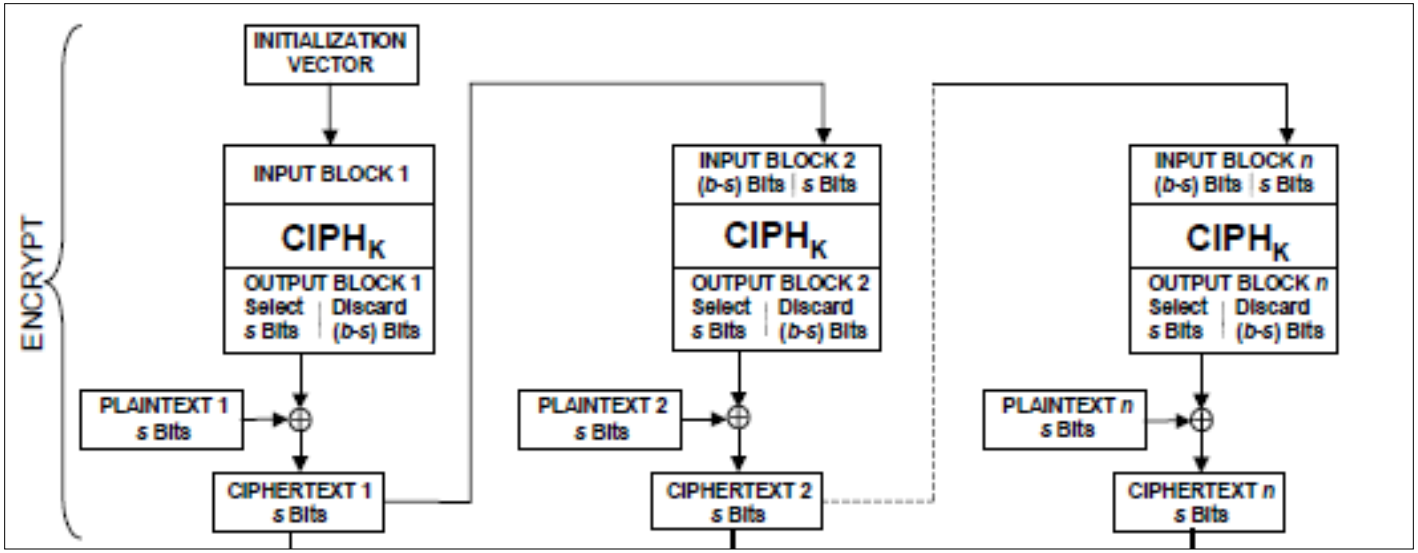
# Block Cipher: Cipher-block Chaining (CBC)

- Ciphertext output from each encrypted plaintext block is used in the encryption for the next block
  - First block encrypted with IV (initialization vector)



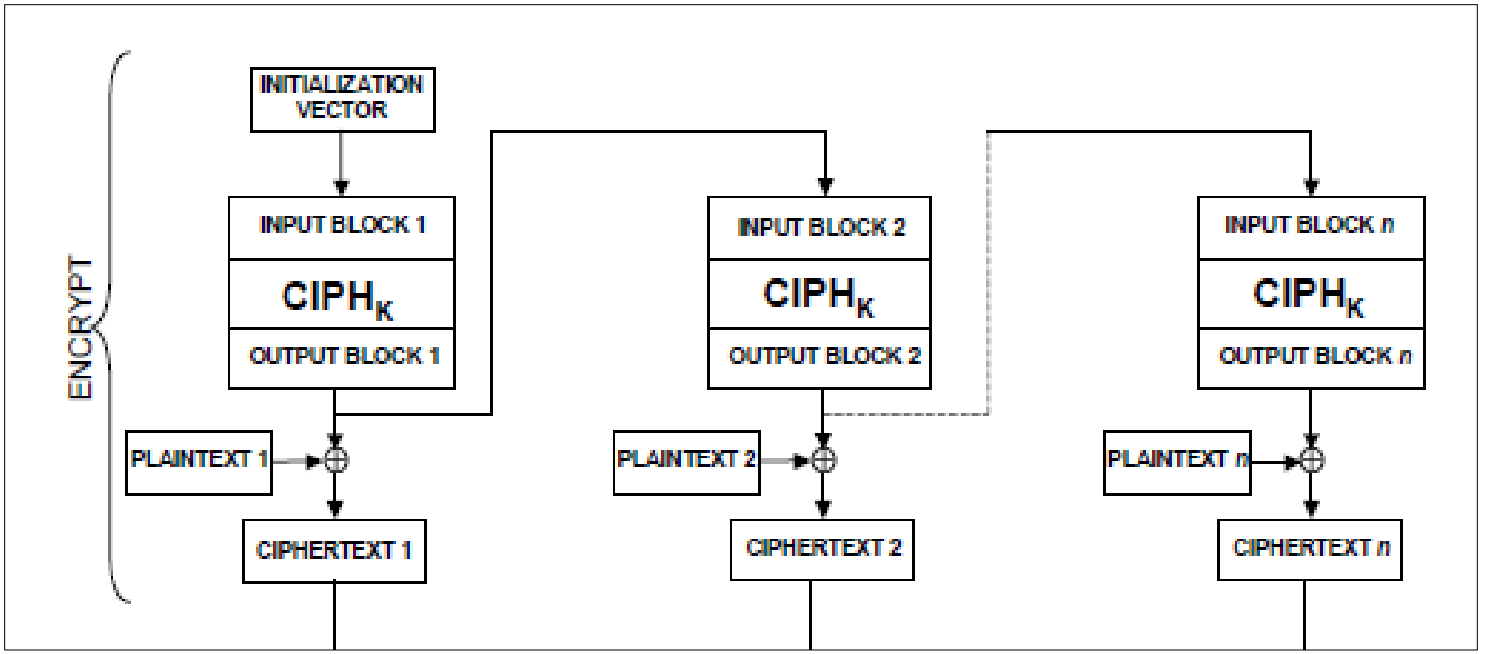
# Block Cipher: Cipher Feedback (CFB)

- Plaintext for block N is XOR'd with the ciphertext from block N-1.
- In the first block, the plaintext XOR'd with the encrypted IV



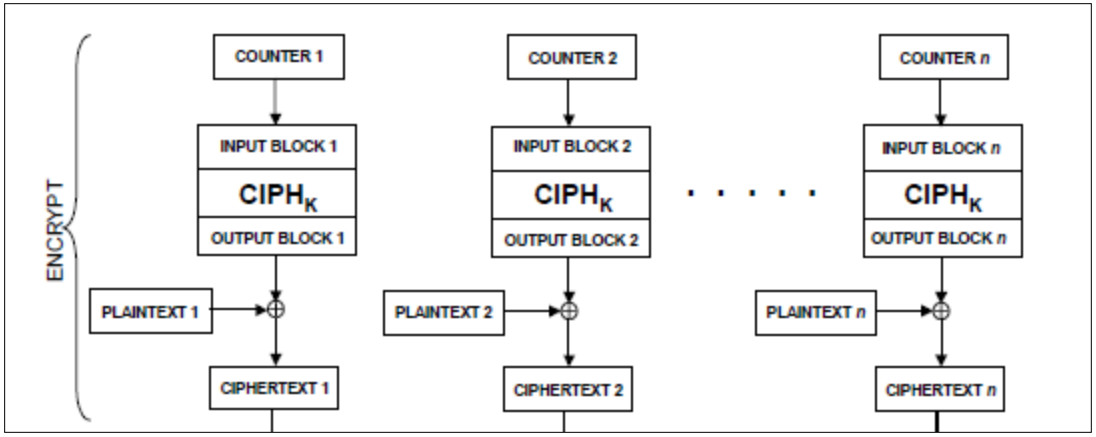
# Block Cipher: Output Feedback (OFB)

- Plaintext is XOR'd with the encrypted material in the previous block to produce ciphertext



# Block Cipher: Counter (CTR)

- Uses a “nonce” (a random number that is used once) that is concatenated with a counter or other simple function, to create a series of keys
  - Allows parallel computation



# Stream Ciphers

- Used to encrypt a continuous stream of data, such as an audio or video transmission
  - A stream cipher is a substitution cipher that typically uses an exclusive-or (XOR) operation that can be performed very quickly by a computer.
- Most common stream cipher is RC4
- Other stream ciphers
  - A5/1, FISH, Phelix1, ISAAC, MUGI, Panama, Phelix, Pike, Sapphire-II. SEAL, SOBER-128, and WAKE

# Stream Ciphers (cont.)

- Encryption: simple XOR with key:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| Key | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| Ciphertext | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |

- Decryption: simple XOR with the same key:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| Key | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| Plaintext | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |

# Types of Encryption Keys

- Symmetric key
  - A common secret that all parties must know
  - Difficult to distribute key securely
  - Used by DES, 3DES, AES, Twofish, Blowfish, IDEA, RC5
- Asymmetric key
  - Public / private key
  - Openly distribute public key to all parties
  - Keep private key secret
  - Anyone can use your public key to send you a message
  - Used by RSA. El Gamal, Elliptic Curve

# Asymmetric Encryption Uses

- Encrypt message with recipient's public key
  - Only recipient can read it, using his or her **private key**
  - Provides **confidentiality**
- Sign message
  - Hash message, encrypt hash with your private key
  - Anyone can verify the signature using your **public key**
  - Provides **integrity** and **non-repudiation** (sender cannot deny authorship)
- Sign and encrypt
  - Both of the above

# Diffie-Hellman Key Exchange

- A way to overcome the problem of exchanging encryption keys without compromising them
  - Based on difficulty of factoring large numbers into prime components

# Length of Encryption Keys

- For symmetric algorithms, use at least 128 bits
- For RSA, use at least 2048 bits
  - 1024 bits no longer recommended by NIST
  - Link Ch 5e

# Protection of Encryption Keys

- Symmetric keys
  - Must be restricted to as few people as possible
  - Protected by a strong password, or encrypted again if needed
- Asymmetric keys
  - Private key requires protection similar to symmetric key
  - Public keys can be published, even on the Internet

# Protecting Keys in Applications

- More difficult to protect keys that applications must be able to access directly
- Hardening techniques
  - Separation of duties
    - Key value known only to operators, not developers or support
  - Store keys in hardware
    - Such as Trusted Platform Module
  - Use of a key encrypting key

# Cryptanalysis

# Cryptanalysis

- Frequency analysis
  - Analyzing frequency of characters in ciphertext
- Birthday attacks
  - Collisions in a hash function can be found in approximately sqrt(N) attempts, where N is the number of possible hash values
  - So SHA-1, 160 bits long, will have a collision in 2^80 values

# Cryptanalysis

- Ciphertext only attack
  - Attacker has only ciphertext
- Chosen plaintext attack
  - Attacker is able to see encryption of selected plaintext
- Chosen ciphertext attack
- Known plaintext attack

# Cryptanalysis (cont.)

- Man in the middle attack
  - Effective against Diffie-Hellman Key Exchange
  - Real public key is replaced by fake one
- Replay attack
  - Effective against SMB, any non-secure cookie-based authentication, almost all Web 2.0 sites

# Applications and Management of Cryptography

# Uses for Cryptography

- File encryption
  - PGP and GPG
  - WinZip (version 9 uses AES)
  - EFS (encrypting file system) for Windows
  - Crypt tool for Unix
- Encrypted volumes and disks
  - Truecrypt for Windows, Mac, Unix
  - Bitlocker for Windows Vista
  - PGP Disk
  - SafeBoot

# Uses for Cryptography (cont.)

- E-mail
  - PGP / GPG – asymmetric key (public key crypto)
  - S/MIME (Secure / Multipurpose Internet Mail Extensions) – certificate based
  - PEM (Privacy Enhanced Mail) – not widely used, requires a single global PKI (which was never implemented)
  - MOSS (MIME Object Security Services) – not widely used

# Uses for Cryptography (cont.)

- Protecting network communications
  - SSH
    - Replacement for telnet, rsh, rlogin
    - Secure FTP
  - IPsec
    - Encrypts all packets between established pairs of hosts
    - Used for VPNs (Virtual Private Networks)
  - SSL/TLS
    - Protects web browser traffic

# Uses for Cryptography (cont.)

- Web browsing – protects session contents from eavesdropping
  - SSL / TLS (Secure Sockets Layer / Transport Layer Security)
    - https: in URL
    - 40-512 bit encryption with secure key exchange
    - Server authentication common, client authentication rare
  - SET (Secure Electronic Transaction)
    - Not widely used

# Key management

# Key Management

- Key creation
  - Process and results must be protected
- Key protection and custody
  - Secured keys in control by the fewest number of persons

# Key Management (cont.)

- Key rotation
  - Periodic update of encryption keys
- Key destruction
  - Securely destroy, to protect encrypted data to be retired
- Key escrow
  - Keys held by a trusted third party

# Message Digests and Hashing

- Message digest or hash
  - The result of a one-way function on a file or message
  - Fixed-length result regardless of message size
  - Impossible (or very difficult) to derive original message from digest
  - No other message should produce the same digest (such pairs are *collisions*)
  - Algorithms
    - MD-5, SHA-1, HMAC

# Error in Textbook

- The book says MD5 is stronger than SHA on page 179—that is ridiculous
- MD5 is weaker than SHA-1, but neither is considered secure any longer
- Official government recommendation: use SHA-2 Instead
  - Links Ch 5f, 5g

# Digital Signatures

- Message digest that is cryptographically combined with signer's private key
  - Requires public key cryptography
  - Verifies message integrity
  - Verifies identity of signer
  - Algorithms: DSA, El Gamal, Elliptic Curve DSA

# Non-repudiation

- Inability for a user to repudiate (deny) an action, because of the methods used to permit or authorize the action
  - Digital signature
    - Verifies integrity of transaction
    - Verifies identity of person performing transaction
  - Password required to use digital signature

# Public Key Infrastructure (PKI)

- Online facility
  - Storage of users' public encryption keys
  - Fast lookup via an API that makes use automatic
  - PKI platforms
    - LDAP
    - Microsoft Active Directory

# Encryption Alternatives

- Steganography
  - Data hidden in image files, subtle changes that the eye won't see; can be encrypted as well
  - Many "stego" tools available
- Watermarking
  - Like a digital signature – a visible or invisible mark that claims ownership