COURSE TECHNOLOGY
CENGAGE Learning™

Principals of Information Security, Fourth Edition

Chapter 8

Cryptography

Do not wait; the time will never be just right. Start where you stand and work with whatever tools you may have at your command, and better tools will be found as you go along.

NAPOLEON HILL (1883–1970) FOUNDER OF THE SCIENCE of SUCCESS

Cryptography

- Cryptology: science of encryption; combines cryptography and cryptanalysis
- Cryptography: process of making and using codes to secure transmission of information
- Cryptanalysis: process of obtaining original message from encrypted message without knowing algorithms
- Encryption: converting original message into a form unreadable by unauthorized individuals
- Decryption: the process of converting the ciphertext message back into plaintext(original message)

Cipher Methods

- Substitution Cipher
- Transposition Cipher
- Book or Running Key Cipher
- Hash Functions

Cryptographic Algorithms

- Often grouped into two broad categories, symmetric and asymmetric
  - Today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations

Symmetric Encryption

- Uses same “secret key” to encipher and decipher message
  - Encryption methods can be extremely efficient, requiring minimal processing
  - Both sender and receiver must possess encryption key
  - If either copy of key is compromised, an intermediate can decrypt and read messages
  - Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES)

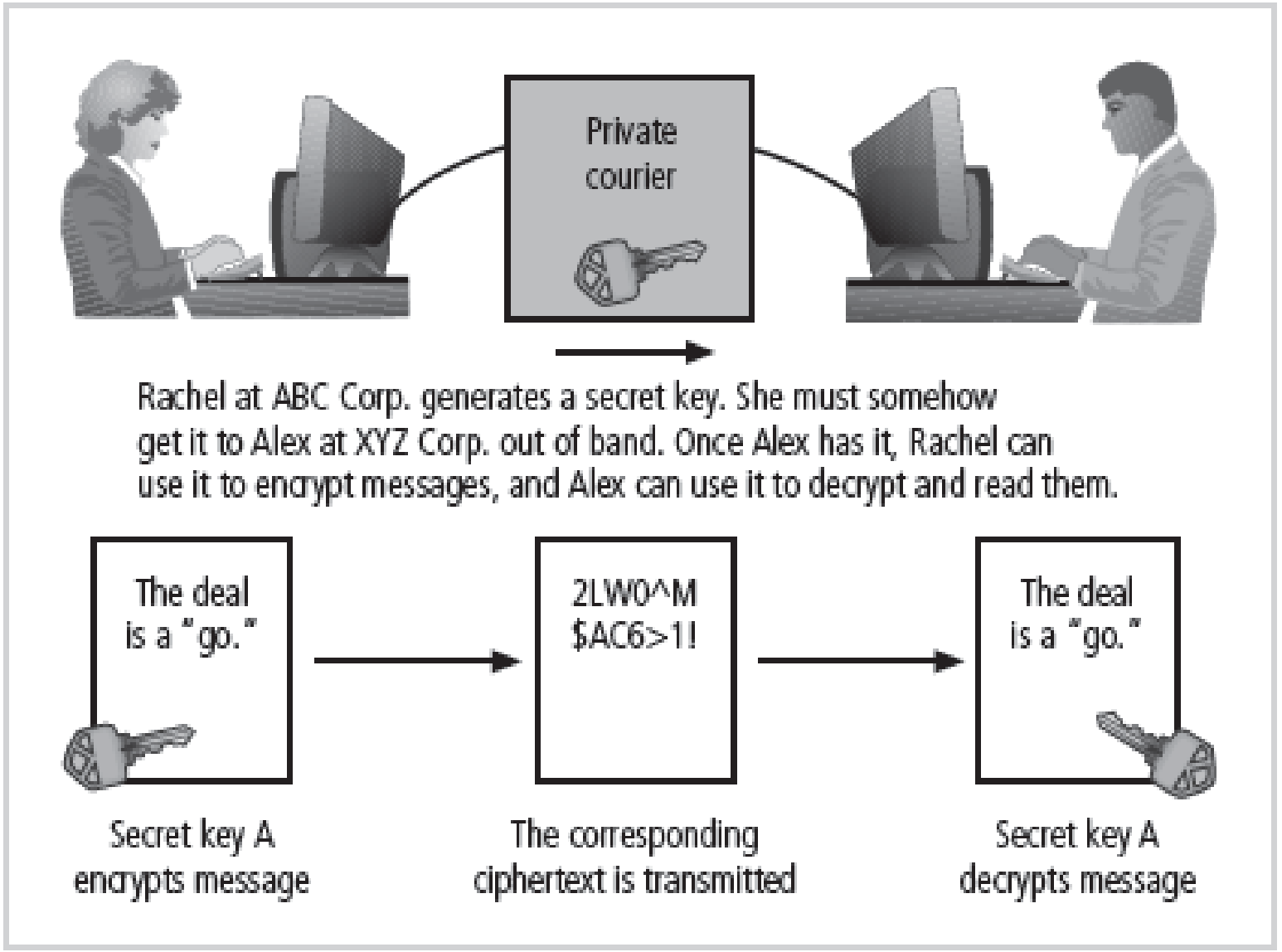

Figure 8-5 Example of Symmetric Encryption

Asymmetric Encryption

- Also known as public-key encryption
- Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - Highest value when one key serves as private key and the other serves as public key
- RSA algorithm

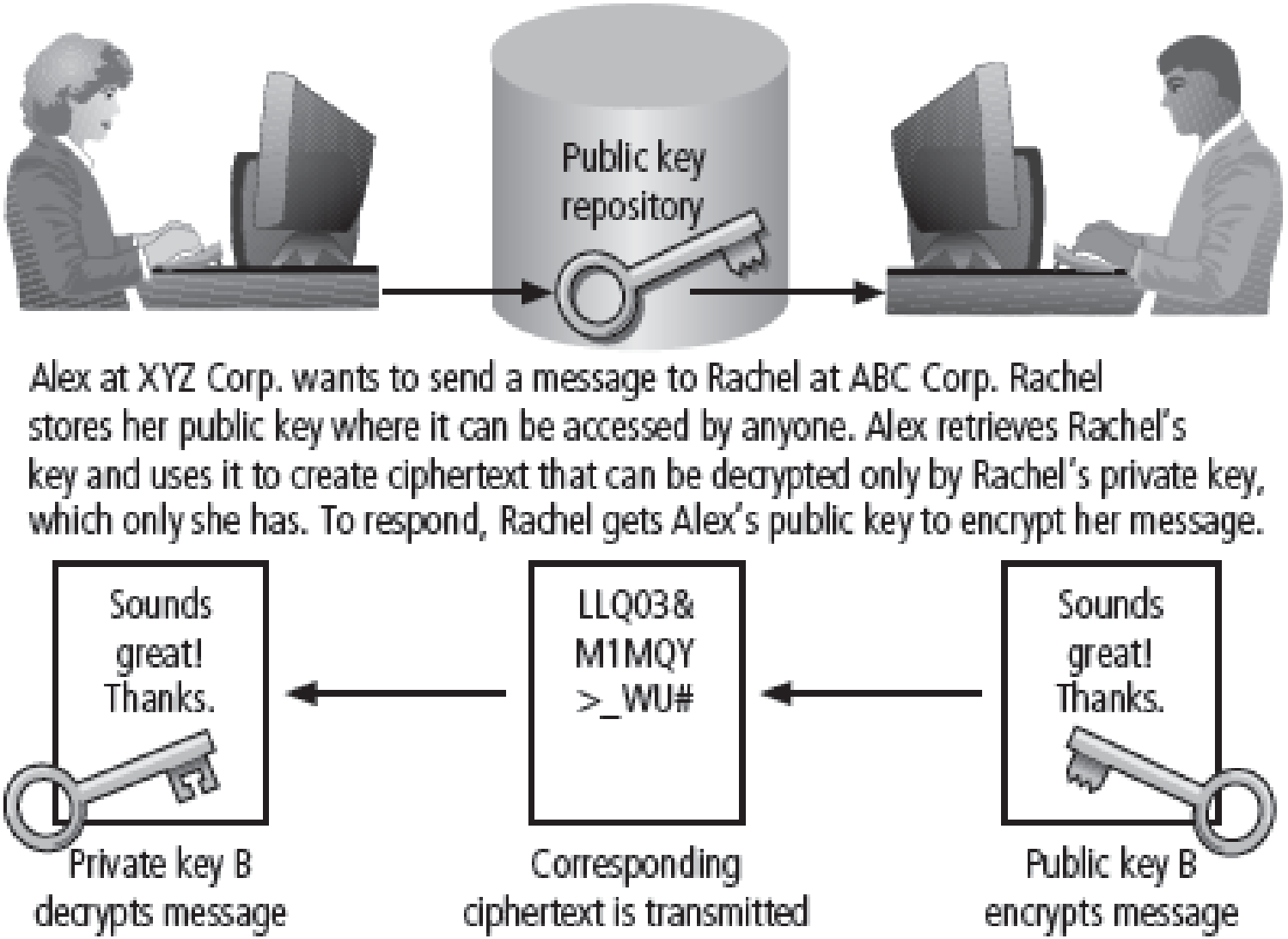

Figure 8-6 Example of Asymmetric Encryption

Encryption Key Size

- When using ciphers, size of cryptovariable or key is very important
- Strength of many encryption applications and cryptosystems measured by key size
- For cryptosystems, security of encrypted data is not dependent on keeping encrypting algorithm secret
- Cryptosystem security depends on keeping some or all of elements of cryptovariable(s) or key(s) secret

Key length (bits)	Maximum Number of Operations (guesses)	Maximum Time to Crack	Estimated Average Time to Crack
8	256	0.0000000085 seconds	0.0000000043 seconds
16	65,636	0.0000022 seconds	0.00000109 seconds
24	16,777,216	0.00056 seconds	0.00028 seconds
32	4,294,967,296	0.143 seconds	0.072 seconds
56	72,057,594,037,927,900	27.800 days	13.9 days
64	18,446,744,073,709,600,000	19.498 years	9.7 years
128	3.40282E+38	359,676,102,360,201, 000,000 years	179,838,051,180,100, 000,000 years
256	1.15792E+77	122,391,435,436,027, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	61,195,717,718,013,400, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years
512	1.3408E+154	14,171,960,013,891,600, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	7,085,980,006,945,820, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years

Table 8-7 Encryption Key Power

Cryptographic Tools

- Potential areas of use include:
  - Ability to conceal the contents of sensitive messages
  - Verify the contents of messages and the identities of their senders
- Tool:
  - Public-Key Infrastructure (PKI)
  - Digital Signatures
  - Digital Certificates

Public-Key Infrastructure (PKI)

- Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems based on public-key cryptosystems
- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation

Digital Signatures

- Verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures
- Nonrepudiation: the process that verifies the message was sent by the sender and thus cannot be refuted

Digital Certificates

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

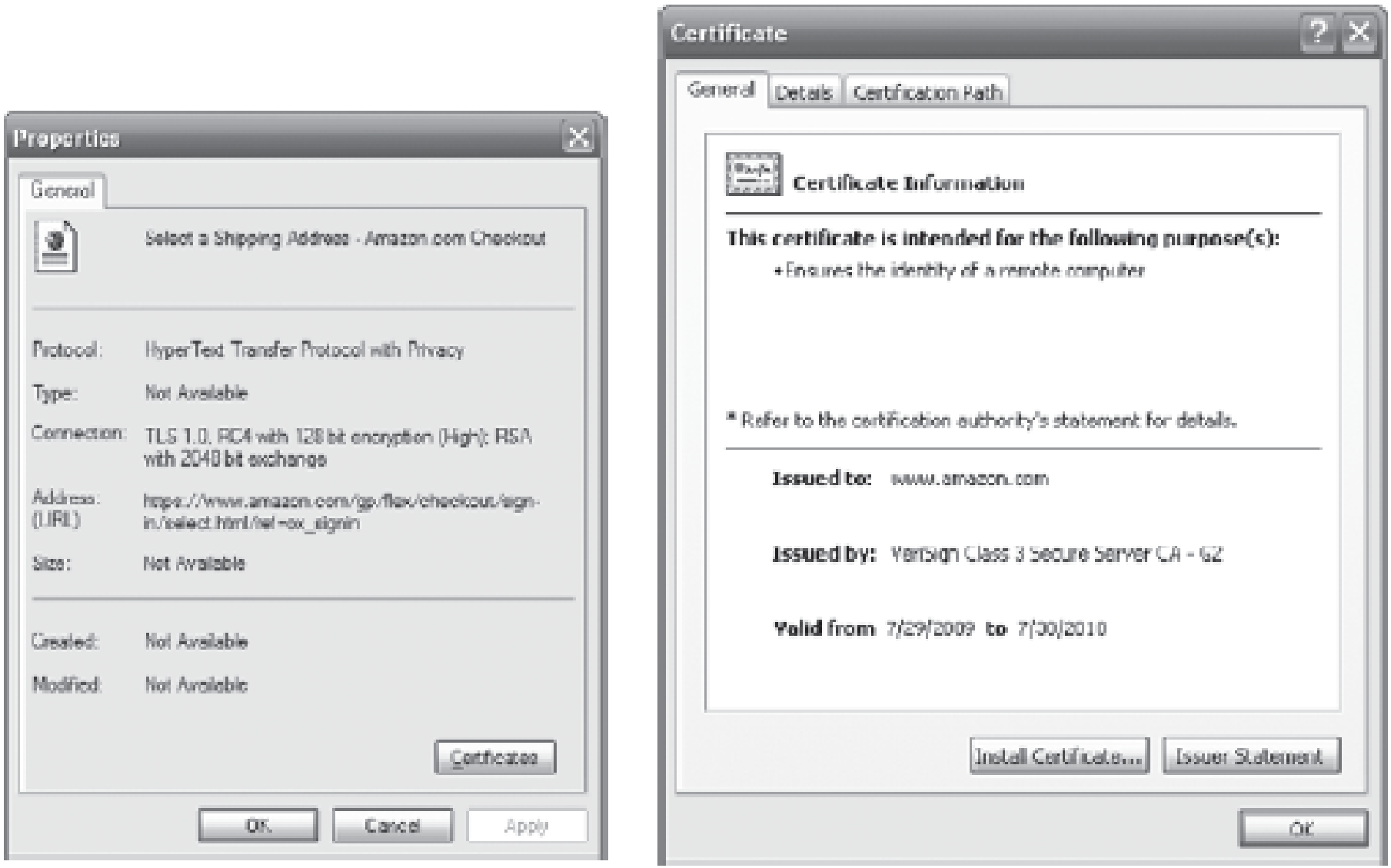

Figure 8-8 Digital Certificate

Steganography

- Process of hiding information
- Has been in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs

Securing Internet Communication with Protocol S-HTTP and SSL

- Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet
- Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet
- S-HTTP is the application of SSL over HTTP

Securing e-mail with S/MIME, PEM, and PGP Protocols

- Secure Multipurpose Internet Mail Extensions (S/MIME): builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
- Privacy Enhanced Mail (PEM): proposed as standard to function with public-key cryptosystems; uses 3DES symmetric key encryption
- Pretty Good Privacy (PGP): uses IDEA Cipher for message encoding

Securing Web transactions with SET, SSL, and S-HTTP

- Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
- Uses DES to encrypt credit card information transfers
- Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP): early attempt to provide security with the 8002.11 network protocol
- Wi-Fi Protected Access (WPA and WPA2): created to resolve issues with WEP
- Next Generation Wireless Protocols: Robust Secure Networks (RSN), AES – Counter Mode Encapsulation, AES – Offset Codebook Encapsulation

Protocols for Secure Communications (continued)

- Securing TCP/IP with IPSec
  - Internet Protocol Security (IPSec): open source protocol to secure communications across any IP-based network

Attacks on Cryptosystems

- Attempts to gain unauthorized access to secure communications have used brute force attacks (ciphertext attacks)
- Attacker may alternatively conduct known-plaintext attack or selected-plaintext attach schemes

Man-in-the-Middle Attack

- Designed to intercept transmission of public key or insert known key structure in place of requested public key
- From victim's perspective, encrypted communication appears to be occurring normally, but in fact, attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Correlation Attacks

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Only defense is selection of strong cryptosystems, thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys

Dictionary Attacks

- Attacker encrypts every word in a dictionary using same cryptosystem used by target
- Dictionary attacks can be successful when the ciphertext consists of relatively few characters (e.g., usernames, passwords)

Timing Attacks

- Attacker eavesdrops during victim's session
  - Uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Once encryption successfully broken, attacker may launch a replay attack (an attempt to resubmit recording of deciphered authentication to gain entry into secure source)

Defending Against Attacks

- No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined
- Key management is not so much management of technology but rather management of people