

# Cryptography

# Terminology (1)

- **Cryptography:**
  - Book definition: process/study of making and using codes to secure information transmission
  - It's really: *the practice/study of rendering information unintelligible to everyone except the intended recipient*
- **Cryptanalysis:** study of obtaining plaintext without knowing key and/or algorithm
- **Cryptology:** study of science of encryption, incl. cryptography
- **Steganography:** process of hiding messages (and the existence thereof) in images, text, etc.
  - See Wayne's book *Disappearing Cryptography* for more info

# Terminology (2)

- **Plaintext:** unencrypted message
- **Ciphertext:** encrypted message
- **Cipher, cryptosystem:** encryption method consisting of algorithm, key, and encryption/decryption procedures
- **Key:** *secret* info used with algorithm to form cipher
- **Kerchhoffs' principle:** a cryptosystem should be secure if everything *but* the key is publicly known
  - Security through obscurity doesn't work!
  - “The enemy knows the system” – Claude Shannon
- **Encrypt:** convert plaintext to ciphertext
- **Decrypt:** convert ciphertext to plaintext

# Terminology (3)

- **Keyspace:** # of values that can be used in a key
  - Ranges of possible and actual values may vary
  - This can greatly affect cipher security
- **Entropy:** # of different *actual* values something can have
  - *Not* keyspace, which specifies total # of *possible* values
  - *Example keyspace:* # of 16-char. passwords using upper-, lowercase letters, numbers, punctuation. If someone always uses 4-char. password, entropy much smaller!
  - Security problems have originated in seeds of pseudo-random number generators with low entropy
- **Work factor:** amount of CPU time needed to analyze ciphertext (get plaintext) *without* knowing key or algorithm
- **Pseudo-random number generator (PRNG):** algorithm that creates “random” number sequence whose properties are similar to those of “real” random number sequences

# Terminology (4)

- **One-way hash function:** converts message to a value (message digest – MD)
  - One-way: can't determine message from MD
  - Examples: MD5, SHA-1, etc.
- **Hash collision:** two messages produce same MD
  - Aim: given a message and an MD, you should not be able to find another message that hashes to same MD
- **Nonce:** number only used once, helps prevent replay attacks

# Cipher Methods (1)

- Plaintext can be encrypted via bit stream or block cipher methods
- **Bit stream:** each plaintext bit transformed into cipher bit one bit at a time
- **Block cipher:** message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key

# Cipher Methods (2)

- **Substitution cipher:** substitute one value for another
- **Monoalphabetic substitution:** uses only one alphabet, *e.g.*, ROT13, Radio Orphan Annie decoder
- **Polyalphabetic substitution:** more advanced; uses two or more alphabets, *e.g.*, Vigenère cipher
- **Transposition cipher:** rearranges values within a block to create ciphertext
- **Exclusive OR (XOR):** Boolean algebra function that compares two bits:
  - If they're identical: result = 0
  - Otherwise: result = 1

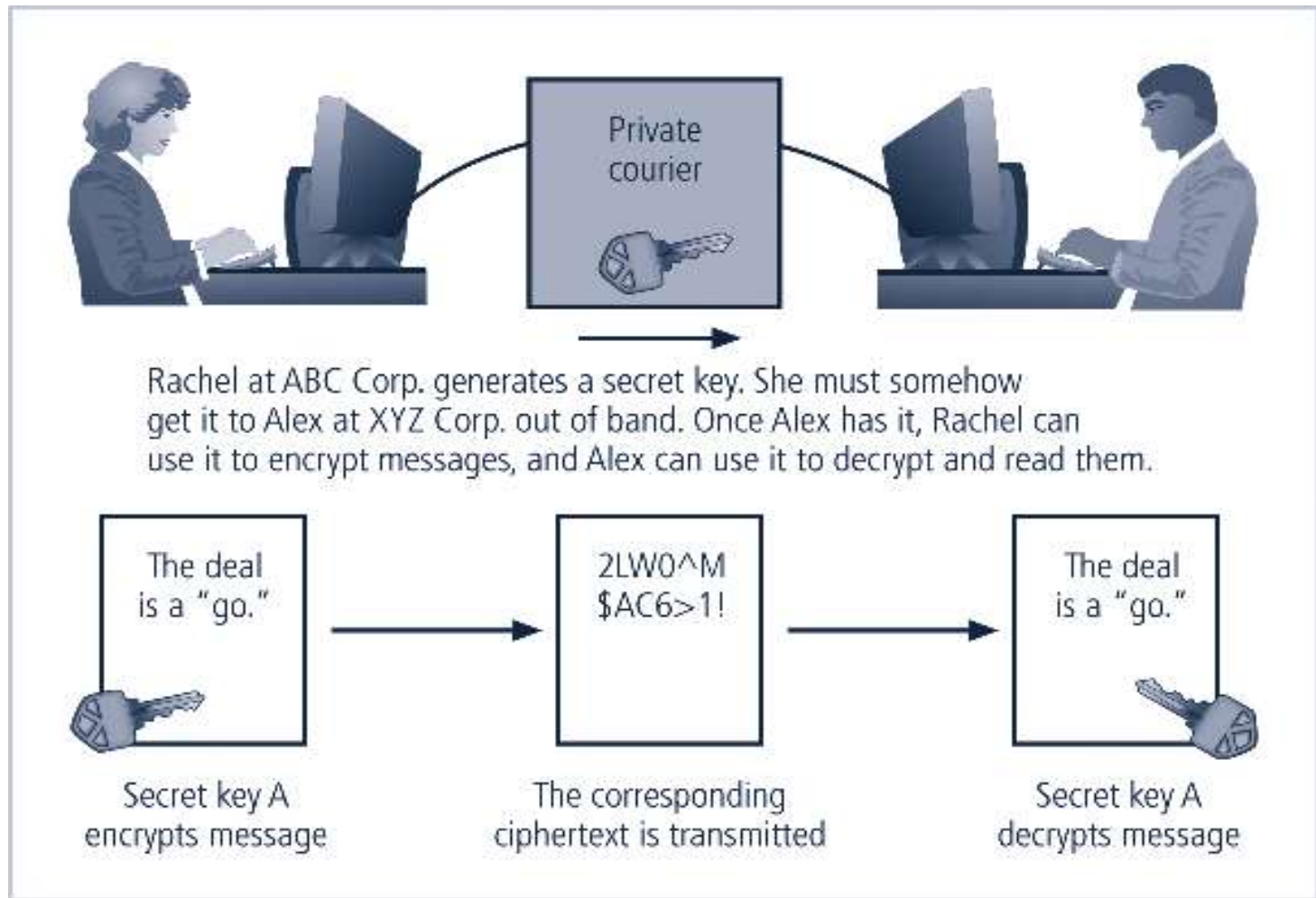
Bit 1	Bit 2	Bit 1 XOR Bit 2
0	0	0
0	1	1
1	0	1
1	1	0

# Cryptographic Algorithms (1)

- Two categories: *symmetric* and *asymmetric*
  - Today's cryptosystems use hybrid combination of both types of algorithms
  - Distinguishing features: #, types of keys used for encryption
- Symmetric: use same “secret key” for message encryption, decryption
  - Computationally efficient
  - Both sender, receiver must have key beforehand
  - If either copy of key is compromised, attacker can decrypt and read messages



# Symmetric Encryption Ex. (Fig. 8.3)



**FIGURE 8-3** Example of Symmetric Encryption

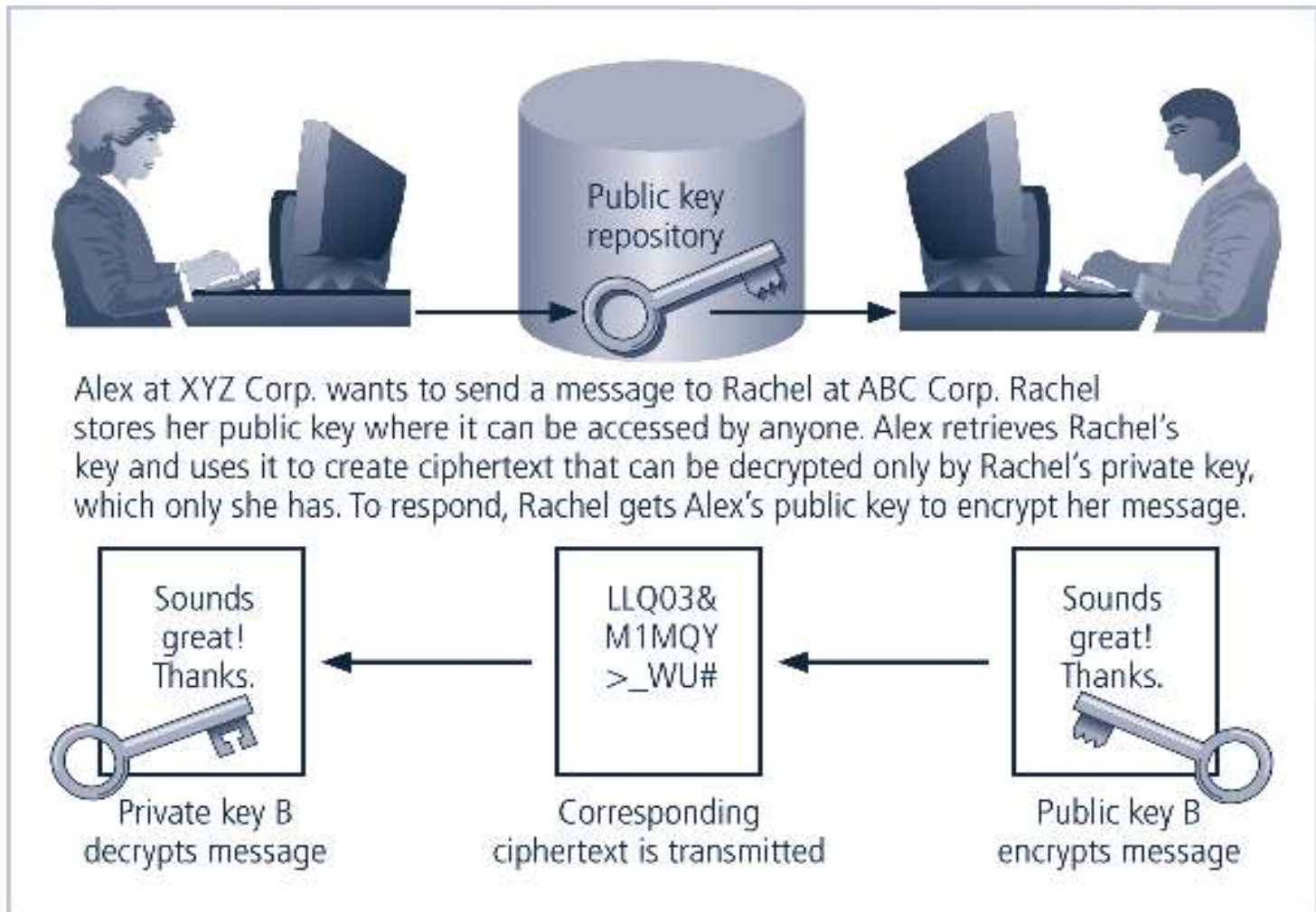
# Cryptographic Algorithms (2)

- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
  - 64-bit block size; 56-bit key
  - Adopted by NIST in 1976 as federal standard for encrypting non-classified information
- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES

# Cryptographic Algorithms (3)

- Asymmetric (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: one key is private, the other is public

# Asymmetric Encryption Ex. (Fig. 8.4)



**FIGURE 8-4** Example of Asymmetric Encryption

# Cryptography Tools

- Public Key Infrastructure (PKI): combination of software, encryption methodologies, protocols, contracts, and third-party services enabling secure communications among users
- PKI systems use public-key encryption
  - Include digital certificates, cert. authorities (CAs)

# Digital Signatures

- Encrypted messages whose authenticity can be mathematically proven
- Created to address need for info. verification in electronic communications (e.g., e-commerce, online healthcare portals, etc.)
- Digital signatures use asymmetric crypto.

# 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

# Protocols for Secure Communications

- Transport Layer Security (TLS): Public-key crypto. protocol for secure HTTP communications
  - Secure Socket Layer (SSL): older protocol that achieves similar purpose
- Email encryption: S-MIME, PGP, GPG
  - Secure Multipurpose Mail Extensions (S-MIME): Adds encryption, authentication to existing mail extensions
  - Pretty Good Privacy (PGP): Free software that encrypts email
  - GNU Privacy Guard (GPG): Similar free tool used on \*nix-like systems



# Summary

- Cryptography provides sophisticated approach to security
  - Many security-related tools use embedded encryption technologies
  - Encryption converts a message into a form that unintended recipients cannot read
- Many tools are available, both symmetric and asymmetric