Cryptography

Modifications by Prof. Dong Xuan
and Adam C. Champion

Learning Objectives

Upon completion of this material, you should be able to:

- Understand the basic cipher methods and cryptographic algorithms
- List and explain the major protocols used for secure communications

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 Wayner'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/encipher:** convert plaintext to ciphertext
- **Decrypt/decipher:** 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 is # of 16-character passwords with upper- and lowercase letters, numbers, punctuation. If someone always uses 4-character password, entropy is much smaller than keyspace
  - Security problems have originated in seeds of pseudo-random number generators with low entropy
- **Work factor:** amount of work (CPU time, instructions) required to perform cryptanalysis on ciphertext to recover 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)

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

Cryptographic Algorithms (2)

- Symmetric encryption: uses same "secret key" to encrypt and decrypt message
  - Encryption methods can be extremely efficient, requiring minimal processing
  - Both sender and receiver must possess key
  - If either copy of key is compromised, an intermediate can decrypt and read messages

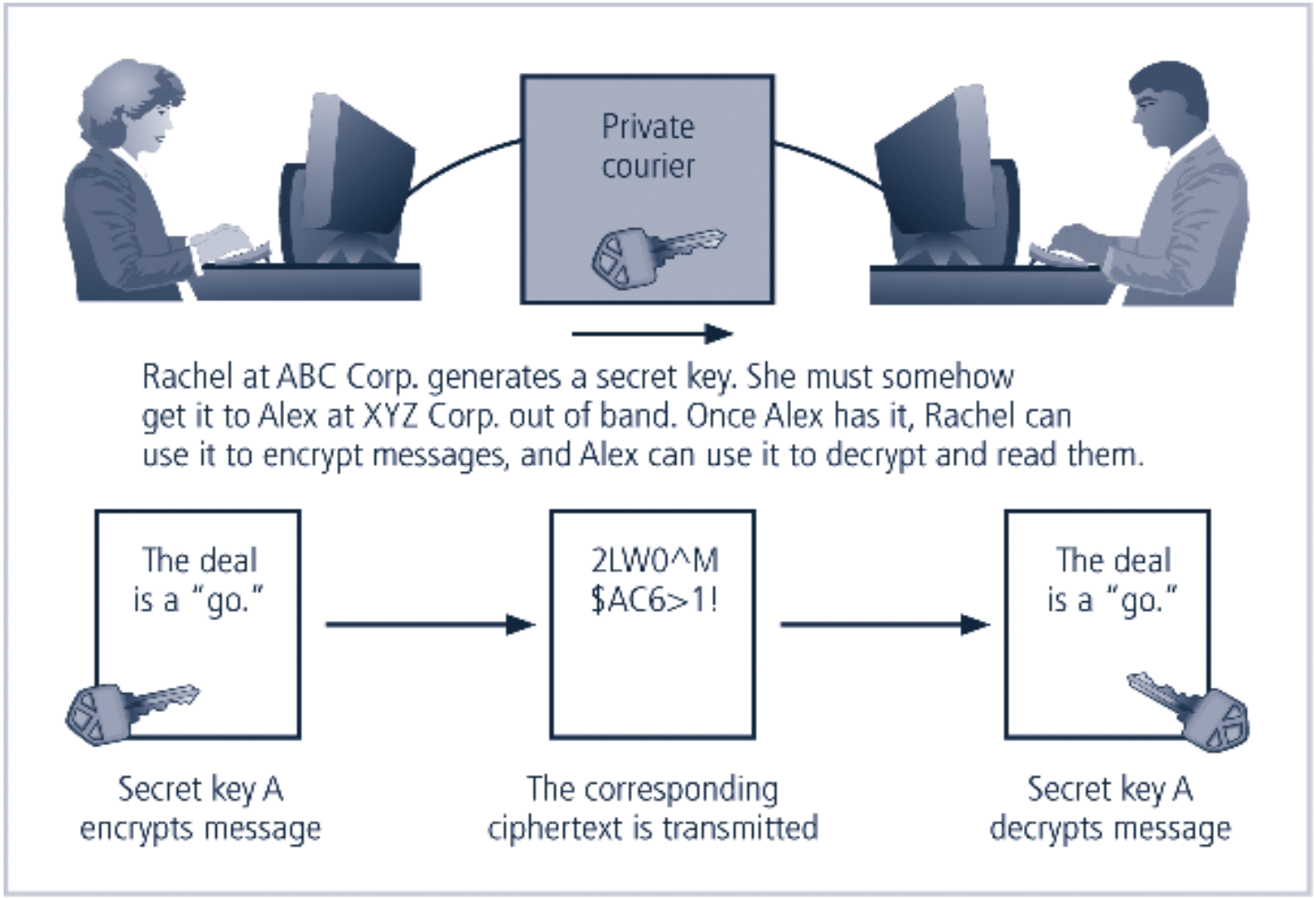


FIGURE 8-3 Example of Symmetric Encryption

Cryptographic Algorithms (3)

- 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 (4)

- Asymmetric Encryption (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 is private key and the other is public key

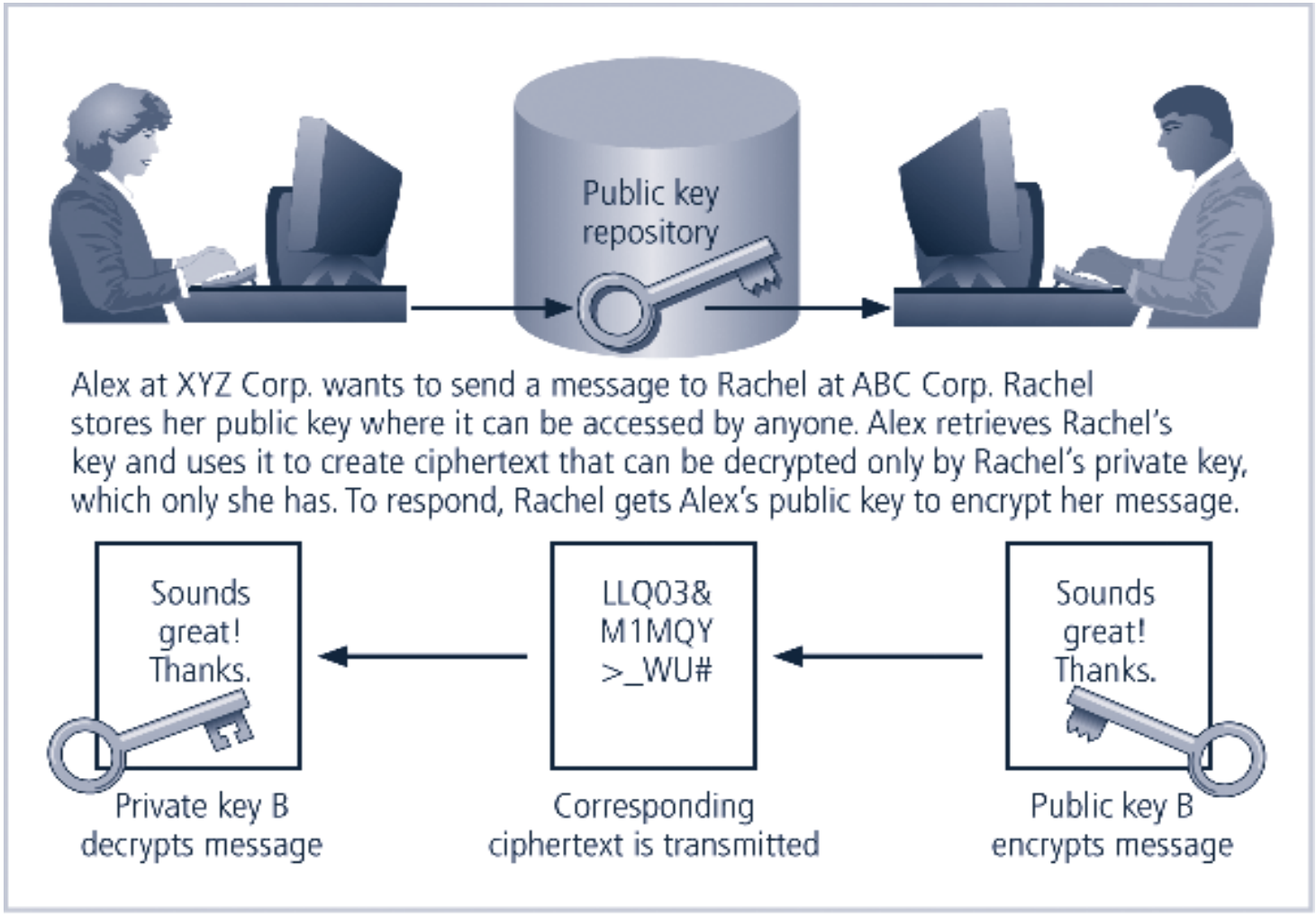


FIGURE 8-4 Example of Asymmetric Encryption

Cryptography Tools

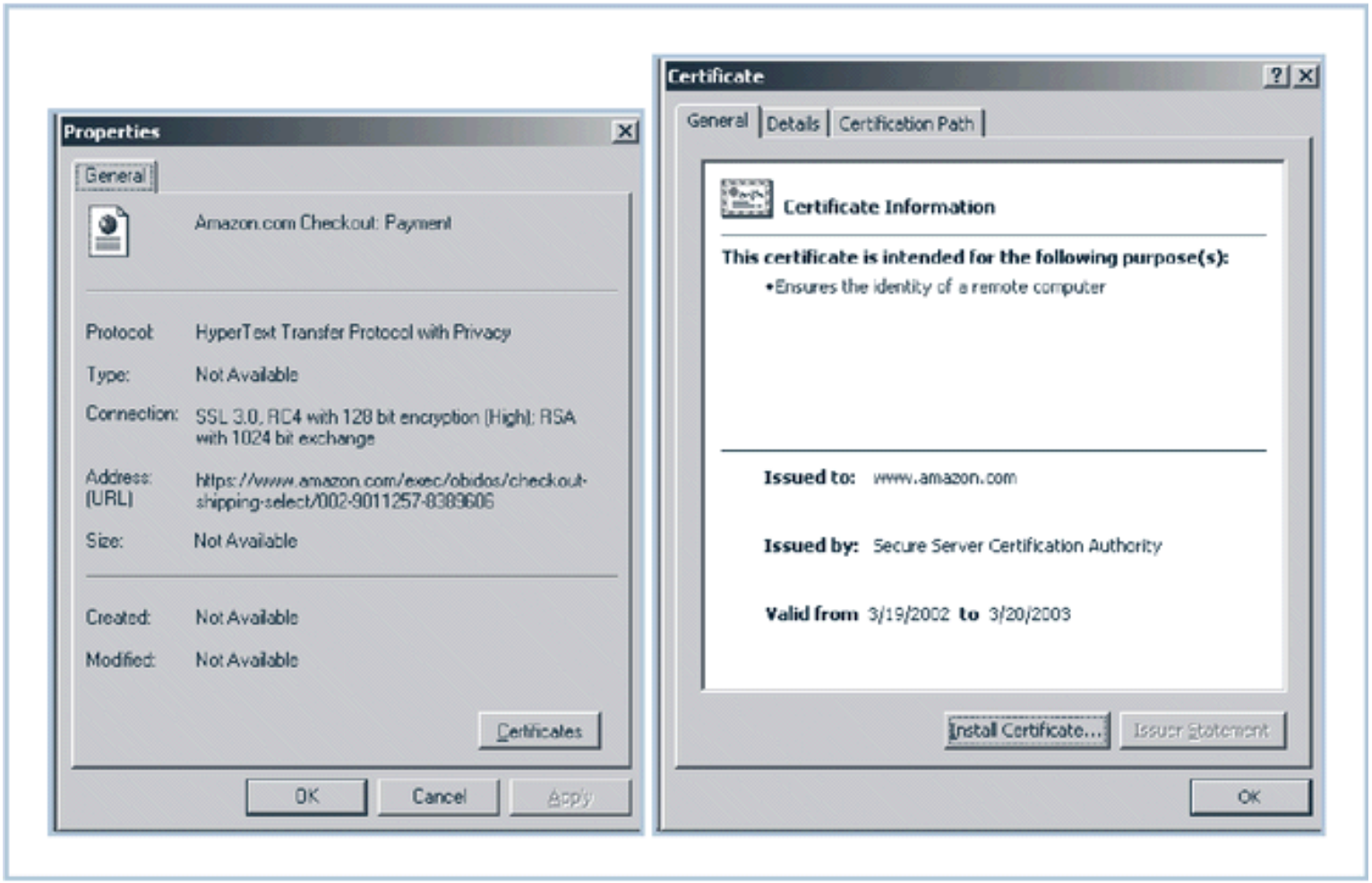
- Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems based on public key cryptosystems, include digital certificates and certificate authorities (CAs)

Digital Signatures

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures

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



Digital Certificates

Protocols for Secure Communications (1)

- 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; allows encryption of information passing between computers through protected and secure virtual connection

Protocols for Secure Communications (2)

- Securing E-mail with S/MIME, PEM, and PGP
  - 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

Protocols for Secure Communications (3)

- 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

Summary

- Cryptography and encryption provide sophisticated approach to security
  - Many security-related tools use embedded encryption technologies
  - Encryption converts a message into a form that is unreadable by the unauthorized
- Many tools are available and can be classified as symmetric or asymmetric, each having advantages and special capabilities