EE 8084
Cyber Security

Cryptography

Yet it may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.

EDGAR ALLAN POE, "THE GOLD BUG"

Learning Objectives

- Chronicle the most significant events and discoveries in the history of cryptology
- Explain the basic principles of cryptography
- Describe the operating principles of the most popular cryptographic tools
- List and explicate the major protocols used for secure communications

Introduction

- Cryptology: science of encryption; encompasses cryptography and cryptanalysis
- Cryptography involves making and using codes to secure messages.
- Cryptanalysis involves cracking or breaking encrypted messages back into their unencrypted origins.

Foundations of Cryptology

- Cryptology has an extensive and multicultural history.
- All popular Web browsers use built-in encryption features for secure e-commerce applications.
- Restrictions on the export of cryptosystems began after WWII.

Terminology

- Must know the following:
  - Algorithm
  - Bit stream cipher
  - Block cipher
  - Cipher or cryptosystem
  - Ciphertext/cryptogram
  - Code
  - Decipher
  - Decrypt
  - Encipher
  - Encrypt
  - Key/Cryptovariable
  - Keyspace
  - Link encryption
  - Plaintext/cleartext
  - Steganography
  - Work factor

Cipher Methods

Plaintext can be encrypted through bit stream or block cipher method.

- Bit stream: Each plaintext bit is transformed into cipher bit one bit at a time.
- Block cipher: Message is 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.

Substitution Cipher

Exchanges one value for another

- Monoalphabetic substitution: uses only one alphabet during encryption process
- Polyalphabetic substitution: more advanced; uses two or more alphabets
- Vigenère cipher: advanced substitution cipher that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

Caesar Cipher – substitution cipher example

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table 8-2 The Vigenère Square

Transposition Cipher

- Simple to understand, but if properly used, produces ciphertext that is difficult to decipher
- Rearranges values within a block to create ciphertext
- Can be done at the bit level or at the byte (character) level
- To make the encryption even stronger, the keys and block sizes can be increased to 128 bits or more.
  - Uses block padding method to facilitate algorithm

Example of transposition cipher

Meet me tomorrow

Exclusive OR (XOR)

- Function of Boolean algebra; two bits are compared and binary result is generated.
  - If two bits are identical, the result is binary 0.
  - If two bits are not identical, the result is binary 1.
- Very simple to implement and simple to break; should not be used by itself when organization is transmitting/storing sensitive data

First bit	Second bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Table 8-3 XOR Table

Vernam Cipher

Uses a set of characters once per encryption process

- To perform:
  - The pad values are added to numeric values that represent the plaintext that needs to be encrypted.
  - Each character of the plaintext is turned into a number and a pad value for that position is added.
  - The resulting sum for that character is then converted back to a ciphertext letter for transmission.
  - If the sum of the two values exceeds 26, then 26 is subtracted from the total.

Vernam cipher – one time pad example

Plain text: Hello

Numerical plaintext:

OTP:

Numerical OTP:

Numerical cipher text:

Ciphertext:

Book-Based Ciphers

Uses text in book as key to decrypt a message

- Book cipher: ciphertext consists of list of codes representing page, line, and word numbers of plaintext word.
- Running key cipher: uses a book for passing key to cipher similar to Vigenère cipher; sender provides encrypted message with sequence of numbers from predetermined book to be used as an indicator block.
- Template Cipher: involves use of hidden message in book, letter, or other message; requires page with specific number of holes cut into it

Hash Functions

- Mathematical algorithms used to confirm specific message identity and that no content has changed
- Hash algorithms: public functions that create hash value
- Use of keys not required
  - Message authentication code (MAC), however, may be attached to a message.
- Used in password verification systems to confirm the identity of the user

Cryptographic Algorithms

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

Symmetric Encryption (1)

Requires same “secret key” to encipher and decipher message; also known as private-key encryption

- Can be programmed into fast computing algorithms and executed quickly
- Both sender and receiver must possess secret key.
- If either copy of key is compromised, an intermediate can decrypt and read messages without sender/receiver knowledge.

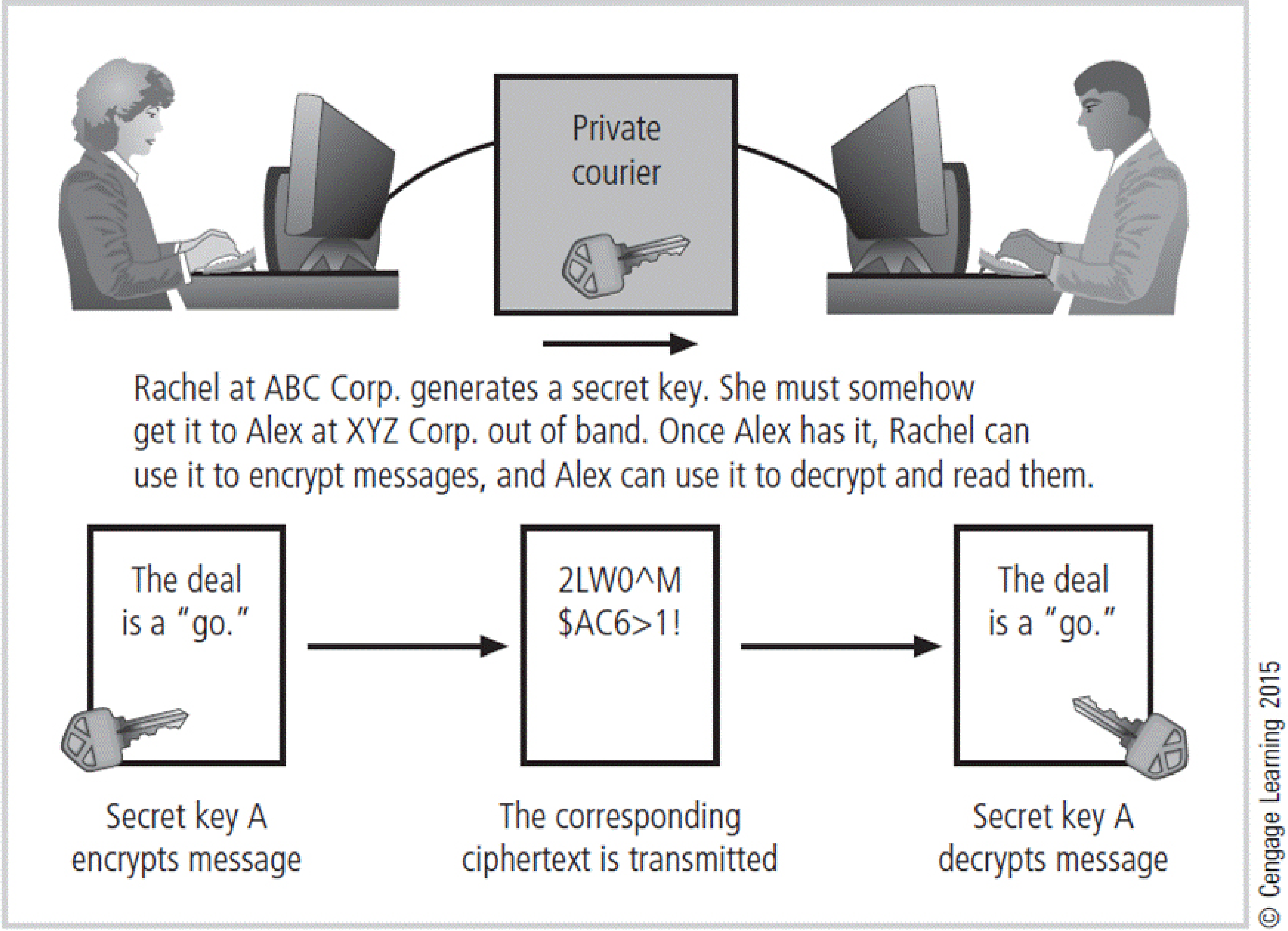

Figure 8-5 Example of symmetric encryption

Symmetric Encryption (2)

- Data Encryption Standard (DES): one of the 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

Asymmetric Encryption

- Also known as public-key encryption
- Uses two different but related keys
  - Either key can encrypt or decrypt a message
  - If Key A encrypts message, only Key B can decrypt
  - Greatest value when one key serves as private key and the other serves as public key
- RSA algorithm was the first public-key encryption algorithm developed/published for commercial use.

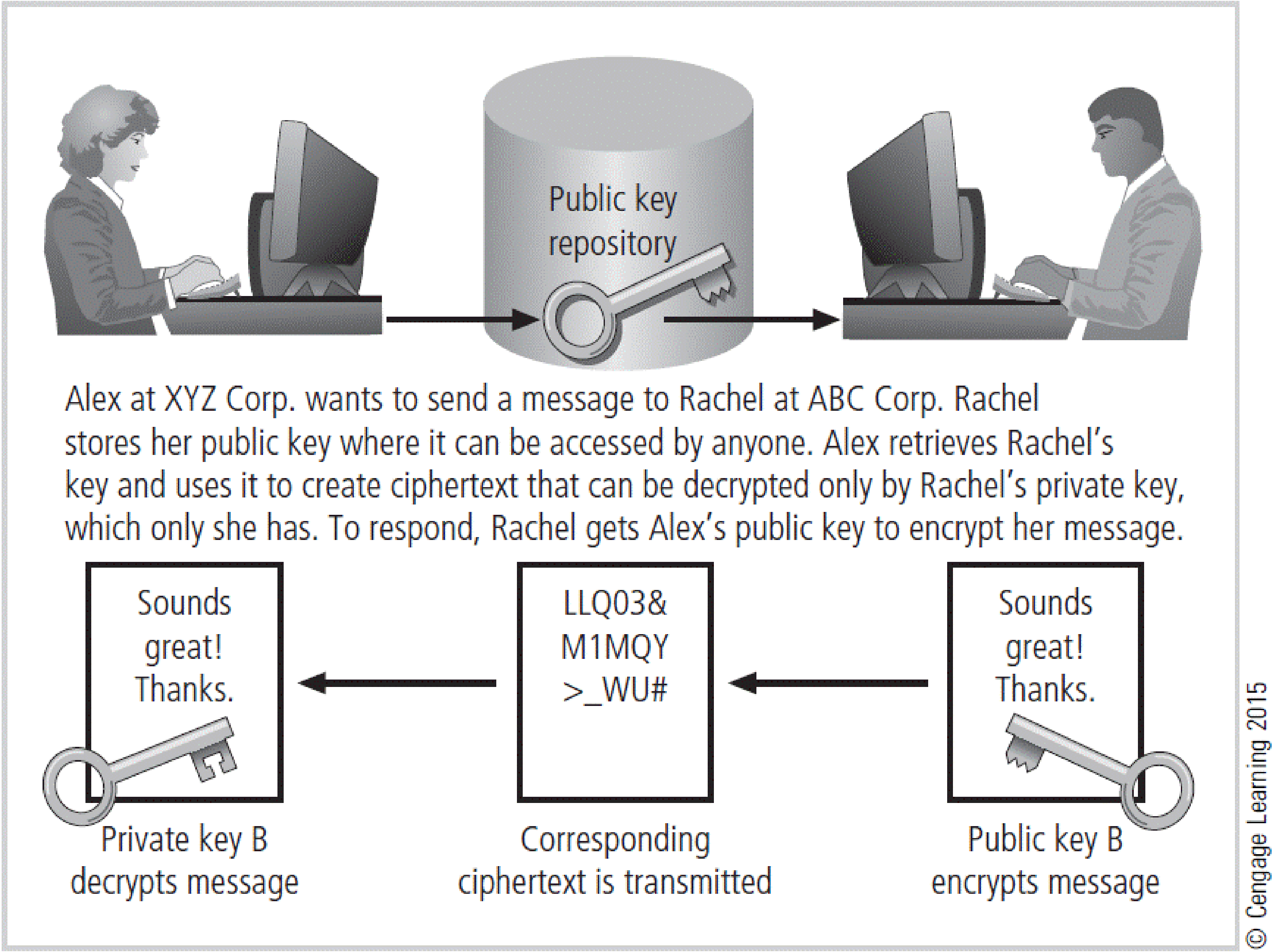

Figure 8-6 Example of asymmetric encryption

Encryption Key Size

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

It is estimated that to crack an encryption key using a brute force attack, a computer needs to perform a maximum of 2^k operations (2^k guesses), where k is the number of bits in the key. In reality, the average estimated time to crack is half that time.

Using an average 2013-era Intel i7 PC (3770K) chip performing 109,924 Dhrystone MIPS (million instructions per second) at 3.9 GHz:

Key length (bits)	Maximum number of operations (guesses)	Maximum time to crack	Estimated average time to crack
16	65,636	0.00000061 seconds	0.00000031 seconds
24	16,777,216	0.00016 seconds	0.00008 seconds
32	4,294,967,296	0.04 seconds	0.02 seconds
56	72,057,594,037,927,900	7.8 days	3.9 days
64	18,446,744,073,709,600,000	5.48 years	2.74 years
128	3.40E+38	101,123,123,702,077, 000,000 years	50,561,561,851,038, 500,000 years
256	1.16E+77	34,410,426,468,960, 700,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	17,205,213,234,480,300, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years
512	1.34E+154	3,984,515,321,402,380, 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, 000,000,000,000,000, 000 years	1,992,257,660,701,190, 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, 000,000,000,000,000, 000 years

Table 8-5 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
- Tools must embody cryptographic capabilities so that they can be applied to the everyday world of computing.

Public-Key Infrastructure (PKI) (1)

- 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

Public-Key Infrastructure (PKI) (2)

- Typical PKI solution protects the transmission and reception of secure information by integrating:
  - A certificate authority (CA)
  - A registration authority (RA)
  - Certificate directories
  - Management protocols
  - Policies and procedures

Digital Signatures

- Created in response to rising the need to verify information transferred via 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 Signature Standard (DSS)

Digital Certificates

- Electronic document/container file containing key value and identifying information about entity that controls key
- Digital signature attached to certificate’s container file certifies file’s origin and integrity
- Different client-server applications use different types of digital certificates to accomplish their assigned functions.
- Distinguished name (DN): uniquely identifies a certificate entity

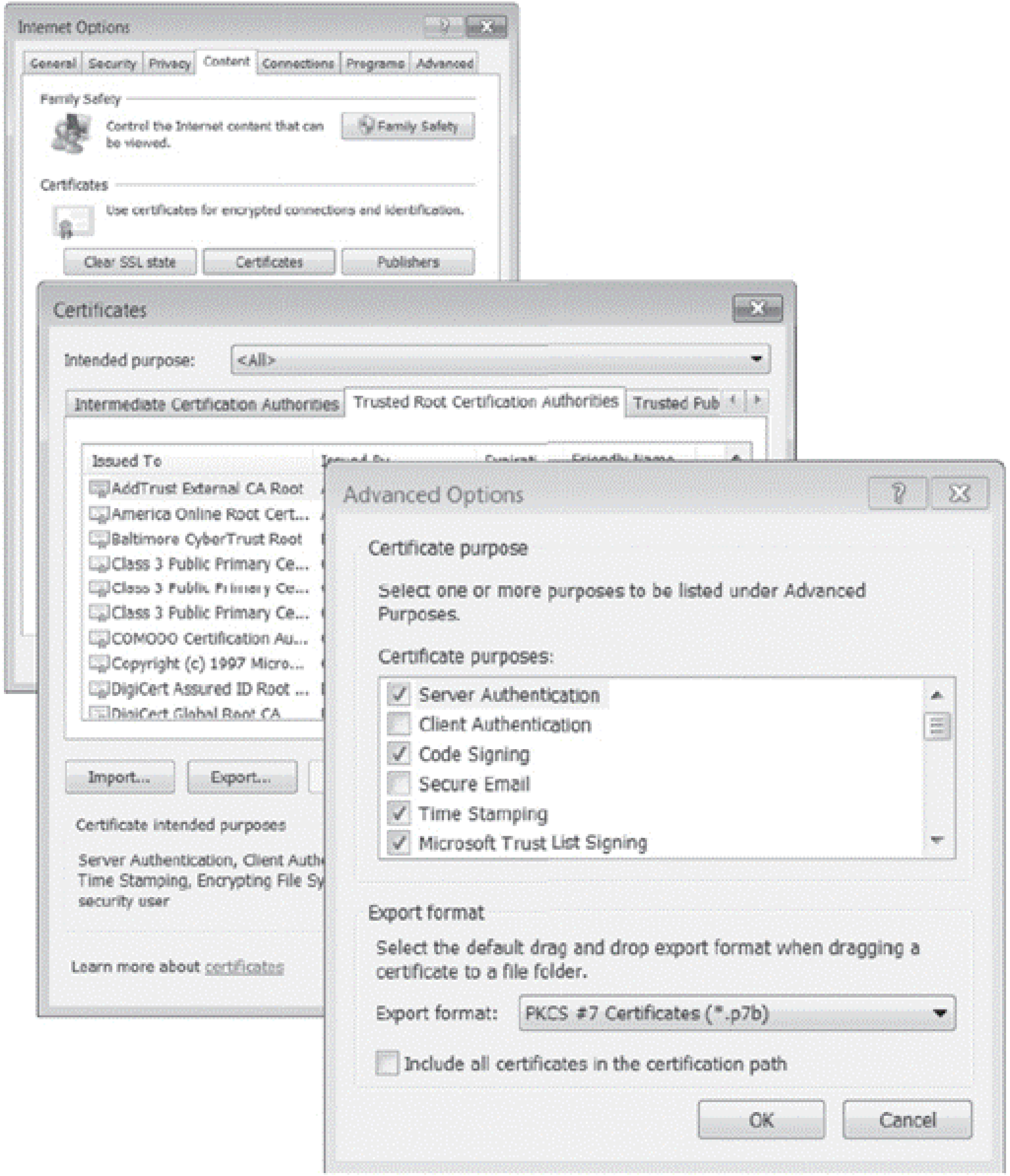

Figure 8-7 Digital signature in Windows 7 Internet Explorer

Source: Windows 7 Internet Explorer.

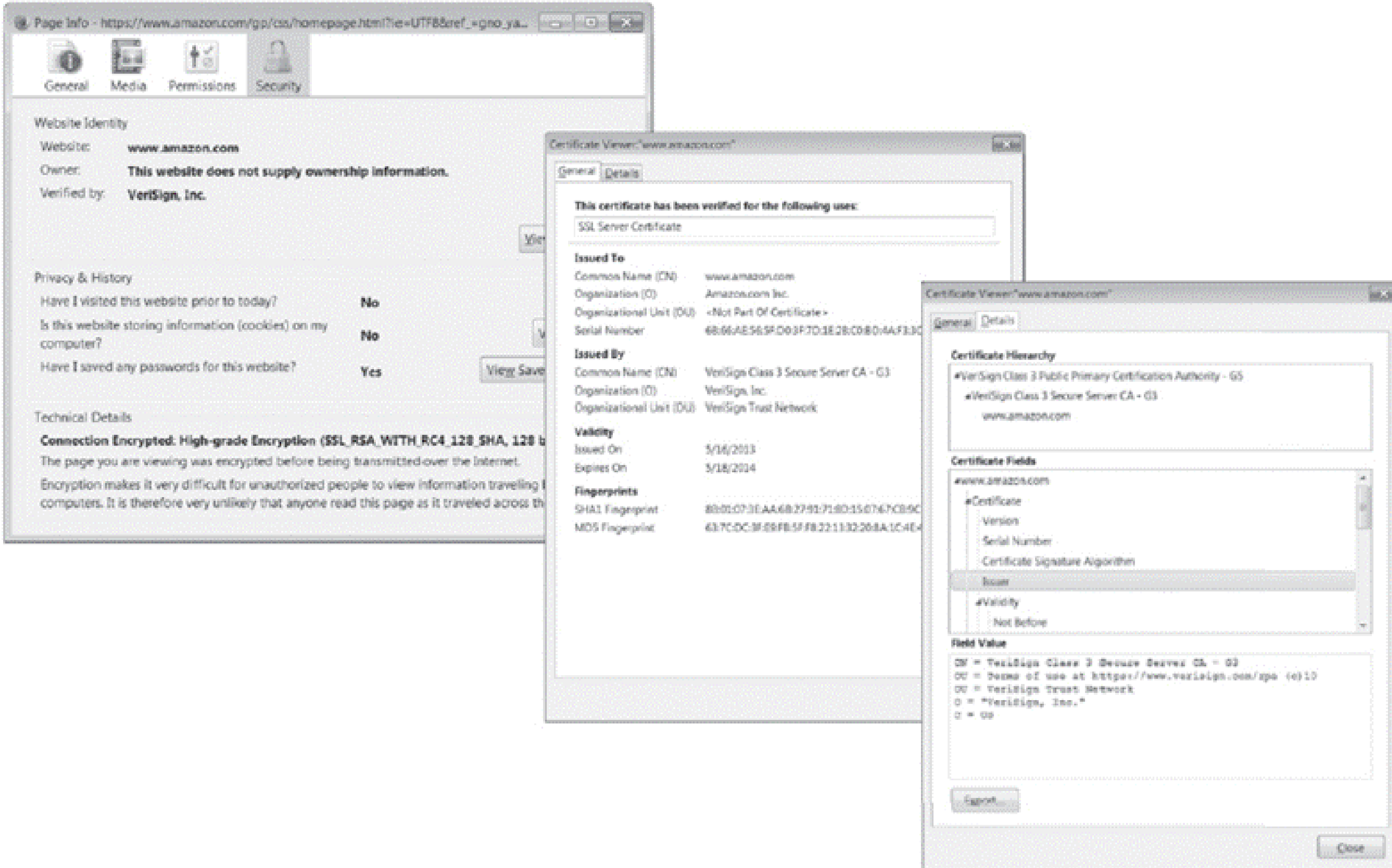

Figure 8-8 Example digital certificate

Source: Amazon.com.

X.509 v3 Certificate structure
Version
Certificate Serial Number
• Algorithm ID • Algorithm ID • Parameters
Issuer Name
• Validity • Not Before • Not After
Subject Name
Subject Public-Key Information • Public-Key Algorithm • Parameters • Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional) • Type • Criticality • Value
Certificate Signature Algorithm
Certificate Signature

Table 8-6 X.509 v3 Certificate Structure[7]

Source: Stallings, W. Cryptography and Network Security, Principles and Practice.

Hybrid Cryptography Systems

- Except with digital certificates, pure asymmetric key encryption is not widely used.
- Asymmetric encryption is more often used with symmetric key encryption, as part of a hybrid system.
- Diffie-Hellman Key Exchange method:
  - Most common hybrid system
  - Provides foundation for subsequent developments in public-key encryption

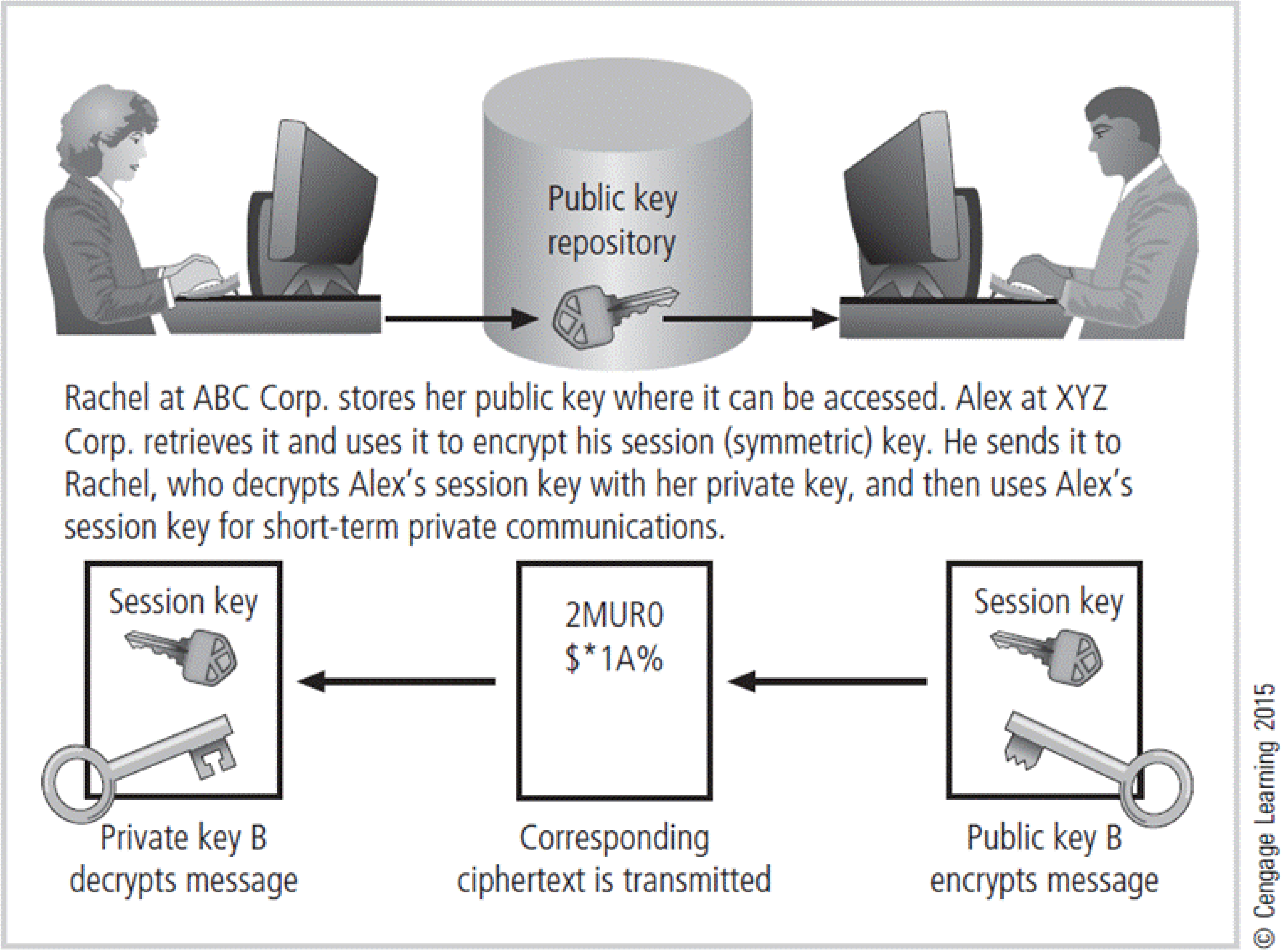

Figure 8-9 Example of hybrid encryption

Steganography

- “Art of secret writing”
- Has been used for centuries
- Most popular modern version hides information within files that 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

Protocols for Secure Communications

- Most of the software currently used to protect the confidentiality of information are not true cryptosystems.
- They are applications to which cryptographic protocols have been added.
- Particularly true of Internet protocols
- As the number of threats to the Internet grew, so did the need for additional security measures.

Securing Internet Communication with S-HTTP and SSL

- Secure Sockets 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

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 and uses digital signatures based on public-key cryptosystems
- Privacy Enhanced Mail (PEM): proposed as standard to use 3DES symmetric key encryption and RSA for key exchanges and digital signatures
- 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 protect against 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 CBC MAC Protocol (CCMP)
- Bluetooth: can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented

	WEP	WPA
Encryption	Broken by scientists and hackers	Overcomes all WEP shortcomings
	40-bit key	128-bit key
	Static key—the same value is used by everyone on the network	Dynamic keys—each user is assigned a key per session with additional keys calculated for each packet
	Manual key distribution—each key is typed by hand into each device	Automatic key distribution
Authentication	Broken; used WEP key itself for authentication	Improved user authentication, using stronger 802.1X and EAP

Table 8-9 WEP Versus WPA

Source: www.wi-fi.org/files/wp_8_WPA%20Security_4-29-03.pdf.

Securing TCP/IP with IPSec and PGP (1)

- Internet Protocol Security (IPSec): an open-source protocol framework for security development within the TCP/IP family of protocol standards
- IPSec uses several different cryptosystems.
  - Diffie-Hellman key exchange for deriving key material between peers on a public network
  - Public key cryptography for signing the Diffie-Hellman exchanges to guarantee identity
  - Bulk encryption algorithms for encrypting the data
  - Digital certificates signed by a certificate authority to act as digital ID cards

IPSec Authentication Header Protocol

Next header	Payload length	Reserved
Security parameters index		
Sequence number		
Authentication data (variable length)		

Next header: Identifies the next higher level protocol, such as TCP or ESP.
Payload length: Specifies the AH content's length.
Reserved: For future use.
Security parameters index: Identifies the security association for this IP packet.
Sequence number: Provides a monotonically increasing counter number for each packet sent. Allows the recipient to order the packet and provides protection against replay attacks.
Authentication data: Variable-length data (multiple of 32 bits) containing the ICV (integrity check value) for this packet.

Encapsulating Security Payload Protocol

Security parameters index		
Sequence number		
Payload data (variable length)		
Padding	Pad length	Next header
Authentication data (variable length)		

Security parameters index: Identifies the security association for this IP packet.
Sequence number: Provides a monotonically increasing counter number for each packet sent. Allows the recipient to order the packets and provides protection against replay attacks.
Payload data: Contains the encrypted data of the IP packet.
Padding: Space for adding bytes if required by encryption algorithm; also helps conceal the actual payload size.
Pad length: Specifies how much of the payload is padding.
Next header: Identifies the next higher level protocol, such as TCP.
Authentication data: Variable-length data (multiple of 32 bits) containing the ICV (integrity check value) for this packet.

Figure 8-10 IPSec headers

Securing TCP/IP with IPSec and PGP (2)

- Pretty Good Privacy (PGP): hybrid cryptosystem designed in 1991 by Phil Zimmermann
  - Combined best available cryptographic algorithms to become open source de facto standard for encryption and authentication of e-mail and file storage applications.
  - Freeware and low-cost commercial PGP versions are available for many platforms.
  - PGP security solution provides six services: authentication by digital signatures, message encryption, compression, e-mail compatibility, segmentation, key management

Summary (1)

- 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.

Summary (2)

- Strength of encryption tool is dependent on the key size but even more dependent on following good management practices.
- Cryptography is used to secure most aspects of Internet and Web uses that require it, drawing on extensive set of protocols and tools designed for that purpose.