COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Network Security
First Edition

Chapter Three
Cryptography

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 explain the major protocols used for secure communications
- Discuss the nature and execution of attacks used against cryptosystems

Introduction

- Critical aspects of cryptography
  - Protecting and verifying transmitted information
- Cryptanalysis
  - Obtaining the original message from an encrypted message without knowing the keys
- Encryption
  - Process of converting an original message into a form unreadable by unauthorized individuals
- Focus of this chapter: general overview

Terminology

- Algorithm
- Cipher or cryptosystem
- Ciphertext or cryptogram
- Code
- Decipher
- Encipher
- Key or cryptovariable
- Keyspace
- Link encryption

Terminology (cont'd.)

- Nonrepudiation
- Plaintext or cleartext
- Steganography
- Substitution
- Transposition
- Work factor

History of Cryptology

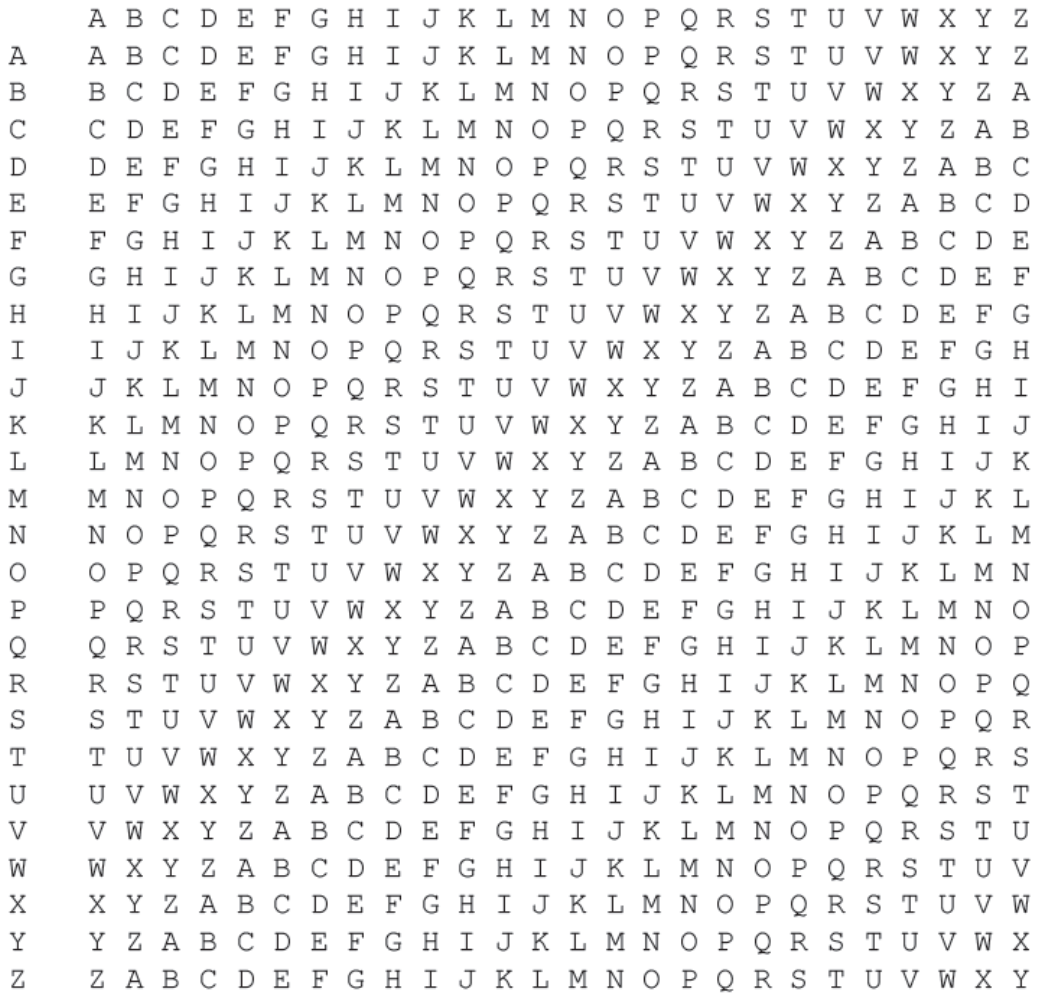
- Egyptians and Mesopotamians used cryptography on clay tablets
- Julius Caesar used a simple substitution cipher to secure military communications
- Alberti used polyalphabetic substitution in 1466
- Thomas Jefferson created the 26-letter wheel cipher
- Used in World War I for radio communications
- Table 3-1 in the text gives detailed history

Cipher Methods

- Bit stream method
  - Each bit in plaintext transformed, one bit at a time
  - Commonly uses exclusive OR operation (XOR)
- Block cipher method
  - Message divided into blocks
  - Each block transformed into an encrypted block
  - Commonly uses substitution, transposition, XOR or combination of these

Substitution Cipher

- One value substituted for another
- Monoalphabetic substitution
  - Uses one alphabet
- Polyalphabetic substitution
  - Uses two or more alphabets
- Caesar cipher
  - Three position shift to the right
- Vigenère cipher
  - See Figure 3-2 for Vigenère square



	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

Figure 3-2 Vigenère Square

© Cengage Learning 2013

Transposition Cipher

- Simple to understand
  - Can product difficult to decipher ciphertext if properly used
- Rearranges values within a block to create ciphertext
  - Bit level or byte level
- Transposition and substitution ciphers can be combined
  - Highly secure encryption process

Exclusive OR Operation

- Exclusive OR (XOR)
  - Function of a binary operation

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Table 3-2 XOR truth table
© Cengage Learning 2013

Vernam Cipher

- Also called one-time pad
- Uses set of characters only one time for each encryption process
- Pad values are added to numeric values that represent plaintext
  - Each character of plaintext turned into a number
  - A pad value for that position is added to it
  - Sum is converted back to a ciphertext character
  - All numbers must be in the range 1-26
- Example on Pages 98-99 of the text

Book or Running Key Cipher

- Text in a book used as key to decrypt a message
- Recipient must know which book is used
  - Page and line number
- Dictionaries and thesauruses commonly used
- Grille cipher
  - Uses a stencil or template with holes cut out
  - Apply template to particular book or document
  - Message is revealed in the holes (apertures)

Hash Functions

- Mathematical algorithms
- Generate a message summary or digest
  - Used to confirm whether message content has changed
  - Confirms message identity and integrity
  - The same message always provides the same hash value
- Hash cannot be used to determine message contents
- Secure Hash Standard (SHS) issued by NIST

Hash Functions (cont'd.)

- Attack methods
  - Rainbow cracking
- Rainbow table
  - Database of precomputed hashes from sequentially calculated passwords
- Protecting against rainbow cracking
  - Protect the file of hashed passwords
  - Limit login attempts
  - Hash salting

Cryptographic Algorithms

- Two broad categories
  - Symmetric
  - Asymmetric
- Today's popular cryptosystems:
  - Combine symmetric and asymmetric algorithms

Cryptographic Notation

- Notation varies depending on the source
- Notation used in this text
  - M represents original message
  - C represents ciphertext
  - E represents the encryption process
  - D represents the decryption process
  - K represents the key
- Example of use: E(M) = C

Symmetric Encryption

- Same secret key used to encipher and decipher the message
- Also called private key encryption
- Mathematical algorithms used
  - Processes executed quickly by computers
- Primary challenge: getting the key to the receiver
  - Must be done “out of band”
    - Using a different channel other than one carrying the ciphertext

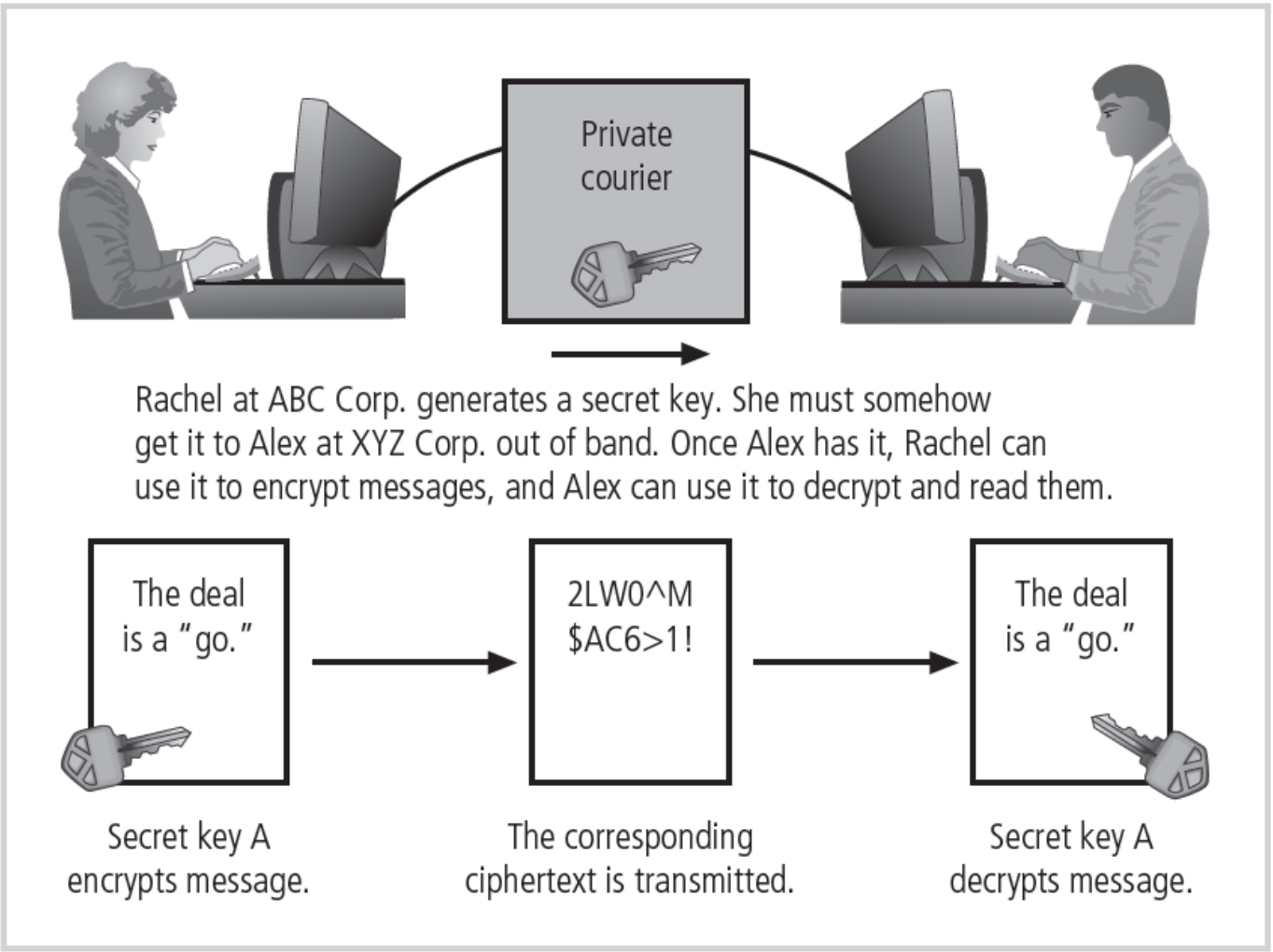


Figure 3-5 Example of symmetric encryption
© *Cengage Learning 2013*

Symmetric Encryption (cont'd.)

- Data Encryption Standard (DES)
  - Developed by IBM
  - Key length: 56 bits
  - Block size: 64 bits
  - Adopted as a federal standard in 1976
- Key length is insufficient to provide acceptable security
  - Electronic Frontier Foundation broke a DES key in 56 hours in 1998

Symmetric Encryption (cont'd.)

- Triple DES (3DES)
  - Provides level of security far beyond DES
  - Uses same encryption
  - Repeats encryption three times
  - Uses three 64-bit keys
  - Common implementations use two or three different keys
- With advances in computing power:
  - Algorithm became too weak to survive

Symmetric Encryption (cont'd.)

- Advanced Encryption Standard (AES)
  - Federal Information Processing Standard (FIPS)
  - Specifies a cryptographic algorithm used within the US government
    - Not used for National Defense
  - Replaces both DES and 3DES
  - Uses the Rijndael Block Cipher
    - Variable block length
    - Key lengths of 128, 192, or 256 bits
  - Number of rounds varies between 9 and 13

Asymmetric Encryption

- Uses two different keys
  - Either key can be used to encrypt or decrypt
- Commonly used with one public key and one private key
  - Public keys shared in reliable directories
  - Private keys kept secret
- RSA
  - Popular asymmetric key cryptosystem
  - Developed in 1977 by Rivest, Shamir, and Adleman

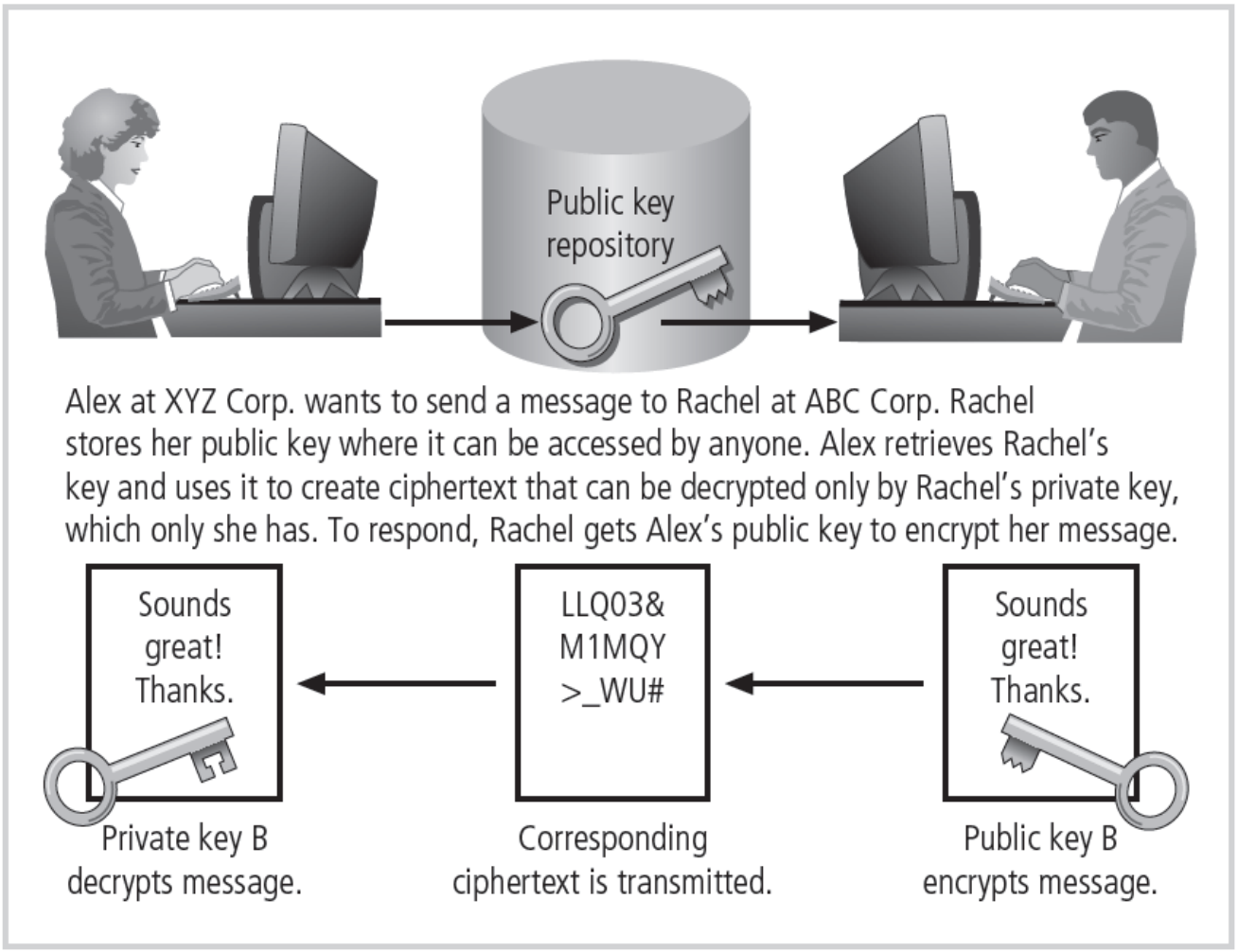


Figure 3-6 Example of asymmetric encryption
© *Cengage Learning 2013*

Hybrid Cryptography Systems

- Problem with asymmetric encryption
  - Holding a two-party conversation requires four keys
- Diffie-Hellman key exchange
  - Exchanging private keys using public-key encryption

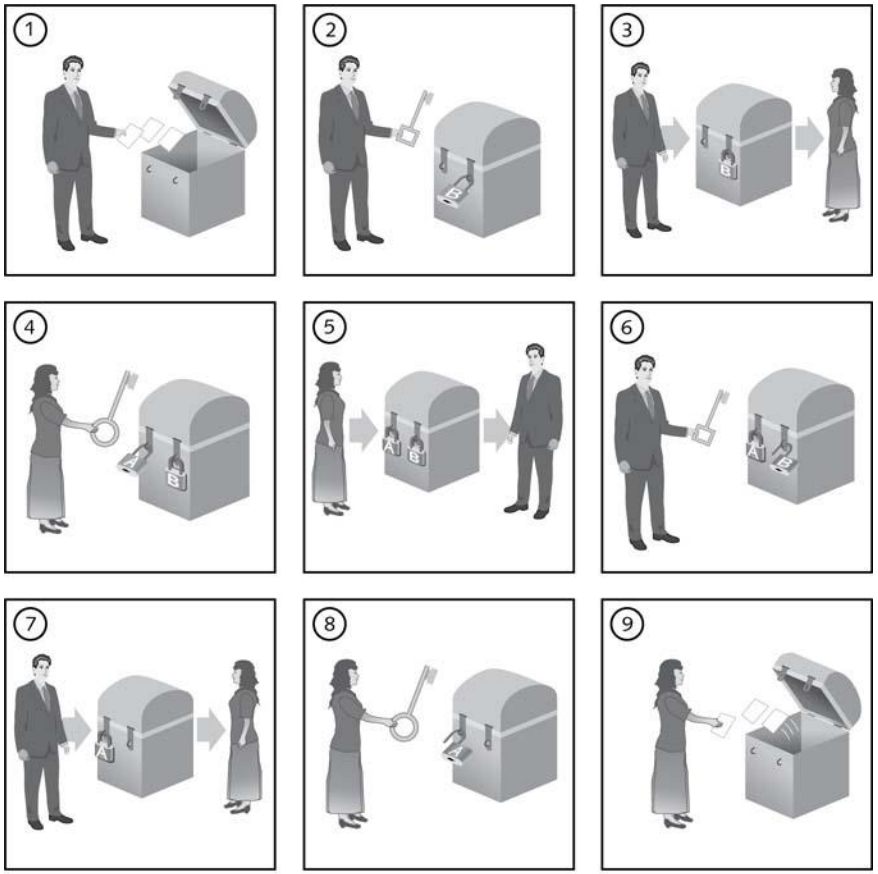


Figure 3-7 Example of Diffie-Hellman key exchange

Figure 3-7 Example of a Diffie-Hellman key exchange
© Cengage Learning 2013

Encryption Key Size

- Strength of the encryption algorithm corresponds to key size
  - Length increases number of random guesses required to break code
- Details of encrypting algorithms typically published
  - Allows research to uncover weaknesses

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	1.844674E+19	19.498 years	9.7 years
128	3.40282E+38	3.596761E+20 years	1.798381E+20 years
256	1.15792E+77	1.2E+59 years	6.1E+103 years
512	1.3408E+154	1.4E+136 years	7.1E+135 years

Table 3-4 Encryption key power
© Cengage Learning 2013

Multiple Encryption Methods

- Using same operation (XOR, substitution, transposition) multiple times
  - No additional benefit gained
- Using different operations (XOR, substitution, transposition)
  - Dramatically scrambles plaintext

Encrypted Communications

- Software systems used to protect information confidentiality
  - Most are not true cryptosystems
  - Applications to which cryptographic protocols have been added
  - Internet protocols fall into this category

Securing Network Communications with IPSec and SSH

- IPSec
  - Open-source protocol
  - Secures communications across IP-based networks
  - Often used to create a secure virtual private network
  - Uses several different cryptosystems
- Components of IPSec
  - IP Security protocol
    - Specifies information to be added to an IP packet
    - Specifies how to encrypt packet data

Securing Network Communications with IPSec and SSH (cont'd.)

- Components of IPSec (cont'd.)
  - Internet Key Exchange (IKE)
    - Uses an asymmetric-based key exchange
- Secure Shell (SSH)
  - Protocol for secure access over an insecure medium
  - Latest version: SSH-2
  - Commonly used to access UNIX and Linux system shells

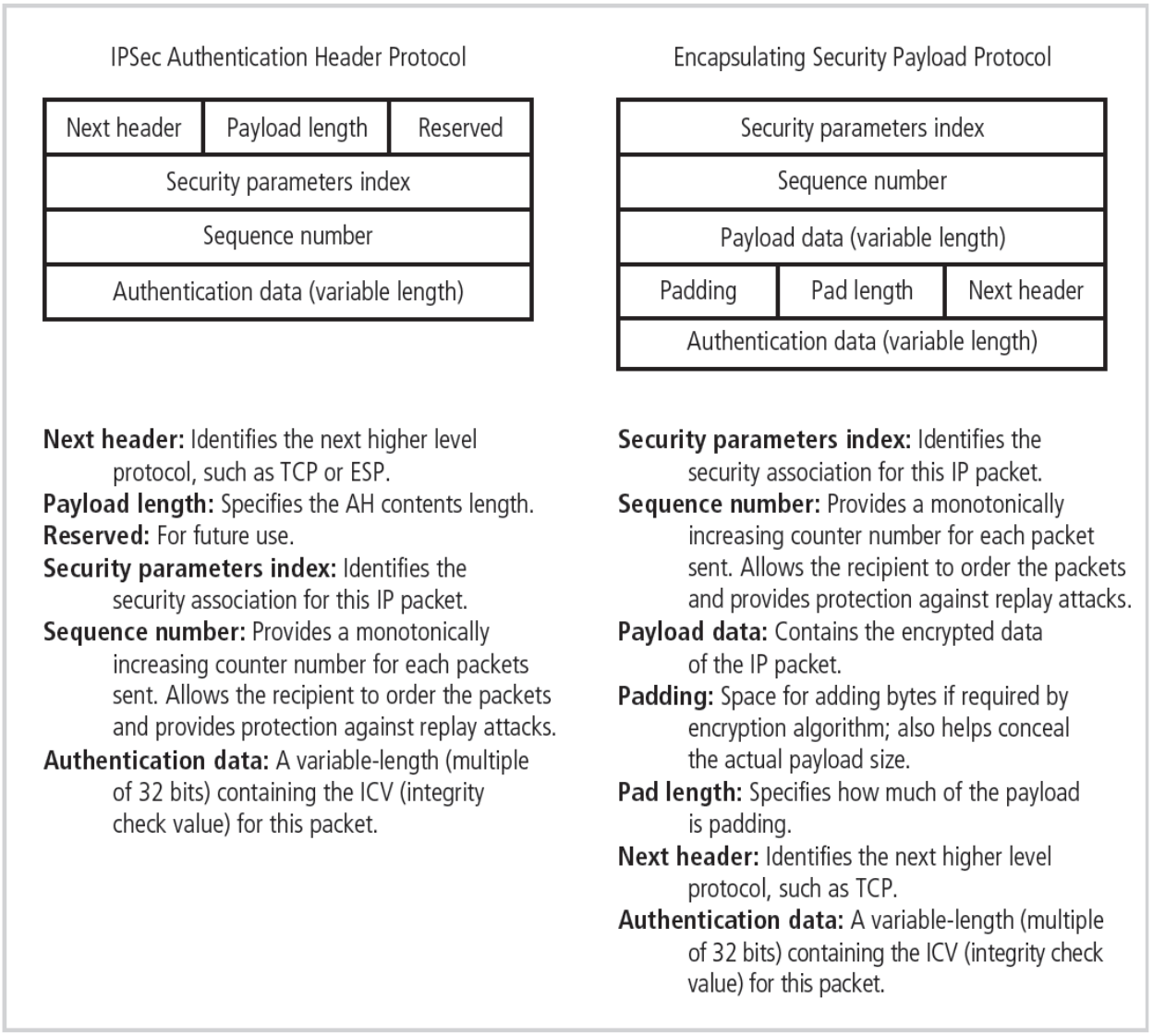


Figure 3-9 IPSec headers

© *Cengage Learning 2013*

Securing Web Communications with SSL and S-HTTP

- Secure Sockets Layer (SSH)
  - Protocol used for public-key encryption
  - Provides a secure channel over the Internet
  - Used in most popular browsers
- Secure HTTP (S-HTTP)
  - Extended version of HTTP
  - Encrypts individual messages transmitted over the Internet
  - Session for each individual data exchange must be established

Securing E-mail with S/MIME and PGP

- SMTP
  - First commonly used Internet e-mail standard
- S/MIME
  - Developed to replace SMTP
  - Handles character sets other than 7-bit ASCII
- Pretty Good Privacy (PGP)
  - Hybrid cryptosystem
  - De facto standard for encryption, authentication for e-mail and file storage applications

Header Field	Function
MIME-version	States conformity to RFCs 2045 and 2046
Content-ID	Identifies MIME entities
Content-type	Describes data in body of message
Content-description	Describes body object
Content-transfer-encoding	Identifies type of conversion used in message body

Table 3-5 MIME message header fields

Securing E-mail with S/MIME and PGP (cont'd.)

- Pretty Good Privacy (cont'd.)
  - Provides six services
    - Authentication using digital signatures
    - Message encryption
    - Compression
    - E-mail compatibility
    - Segmentation
    - Key management

Securing Wireless Networks with WEP and WPA

- Wireless LANs
  - Inherently insecure
  - Must use some form of cryptographic security control
- Two protocols in wide use
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)

Securing Wireless Networks with WEP and WPA (cont'd.)

- Wired Equivalent Privacy (WEP)
  - Early attempt to provide security with 802.11 network protocol
  - Considered weak today
- Wi-Fi Protected Access (WPA and WPA2)
  - Created to resolve issues with WEP
  - 128-bit key size
  - Uses dynamically changing keys
    - Created and shared by authentication server

	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, utilizing stronger 802.1X and EAP

Table 3-8 Comparison of WEP and WPA
Source: Wi-Fi Alliance
© Cengage Learning 2013

Next-Generation Wireless Protocols

- Robust Secure Networks (RSN)
  - Planned replacement for Temporal Key Integrity Profile (TKIP) in WPA
  - Supports key lengths up to 256 bits
  - Not compatible with older hardware

Cryptographic Tools

- Cryptographic capabilities
  - Must be embodied in tools
  - Apply cryptology to everyday computing
- Public Key Infrastructure
  - Integrated system of software, services, and encryption
- Digital certificates
  - Public-key container files
  - Allow computer programs to validate keys
    - Identify key owners

Public Key Infrastructure (PKI)

- Typical PKI solution components
  - Certificate authority (CA)
  - Registration authority (RA)
  - Certificate directories
  - Management protocols
  - Policies and procedures
- Certificate authority
  - Provides housekeeping activities associated with keys and certificates
  - Distributes certificate revocation list (CRL)

Digital Signatures

- Encrypted messages that can be mathematically proven authentic
- Management of digital signatures
  - Built into most Web browsers
  - Based on Digital Signature Standard

Digital Certificates

- Electronic document or container file that holds:
  - Key value
  - Identifying information about key owner
- Authenticate cryptographic key embedded in a certificate
- Often issued and certified by a third party (CA)
- Verification process occurs when downloading software via the Internet

Steganography

- The art of secret writing
- Technically, not a form of cryptography
- Another way of protecting information confidentiality in transit
- Most popular modern version
  - Hiding information within image files

Attacks on Cryptosystems

- Brute force attacks
  - Hacker searches for clues in ciphertext
    - Frequency analysis
- Known-plaintext attack
- Selected-plaintext attack

Man-in-the-Middle Attack

- Attempts to intercept a public key
- Attempts to insert known key structure in place of public key
- Prevention strategy
  - Establish public key with digital signature
  - Attacker cannot duplicate signature

Correlation Attacks

- Collection of brute force methods
- Attempt to deduce statistical relationships between unknown key and ciphertext
- Advanced codebreaking methods
  - Differential and linear cryptanalysis

Dictionary Attacks

- Attacker encrypts every word in a dictionary
  - Applies same cryptosystem used by target
  - Looks for match between target ciphertext and list of encrypted words
- Successful with small files
  - Files containing usernames and passwords

Timing Attacks

- Attacker eavesdrops on victim's session
- Uses statistical analysis of patterns to discern information
- Can be used to gain information about encryption key
  - Can eliminate some algorithms and narrow search

Defending Against Attacks

- Encryption
  - Useful tool to protect information confidentiality
  - Process of hiding the true meaning of information
  - Inherent flaw
    - If you discover the key, you can read the message
  - Key management is important

Summary

- Encryption is the process of converting a message to a form unreadable by unauthorized individuals
- Strength of encryption systems is generally determined by the key length
- Hash functions generate a message summary that can confirm message has not been altered
- Digital signatures are encrypted messages verified by a third party
- Attacks on information often use brute force methods