Principles of Information Security

Chapter 8
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

- Upon completion of this material, you should be able to:
  - 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
  - Discuss the nature and execution of the dominant methods of attack used against cryptosystems

2

Introduction

- 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

3

Foundations of Cryptology

- Cryptology has a long and multicultural history
- With emergence of technology, need for encryption in information technology environment greatly increased
- All popular Web browsers use built-in encryption features for secure e-commerce applications

4

Cipher Methods

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

5

Substitution Cipher

- Substitute one value for another
- Monoalphabetic substitution: uses only one alphabet
- Polyalphabetic substitution: more advanced; uses two or more alphabets
- Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

6

Transposition Cipher

- Easy 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 made much larger

8

Exclusive OR (XOR)

- Function of Boolean algebra; two bits are compared
  - If two bits are identical, result is binary 0
  - If two bits not identical, result is binary 1
- A very simple symmetric cipher that is used in many applications where security is not a defined requirement

9

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

Table 8-3 XOR Truth Table

10

Book or Running Key Cipher

- Uses text in book as key to decrypt a message
- Ciphertext contains codes representing page, line, and word numbers
- Algorithm is the mechanical process of:
  - Looking up the references from the ciphertext
  - Converting each reference to a word by using the ciphertext's value and the key
- Typical sources are dictionaries and thesauruses

12

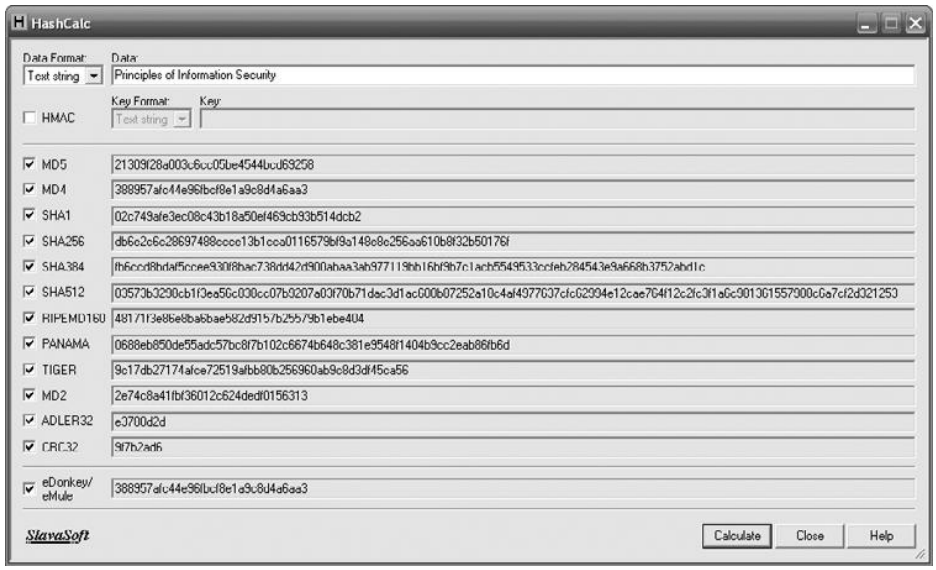

Figure 8-4 Various Hash Values

13

Hash Functions

- Mathematical algorithms that generate message summary/digest to confirm message identity and confirm no content has changed
- Hash algorithms: publicly known 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 identity of user

14

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

15

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

16

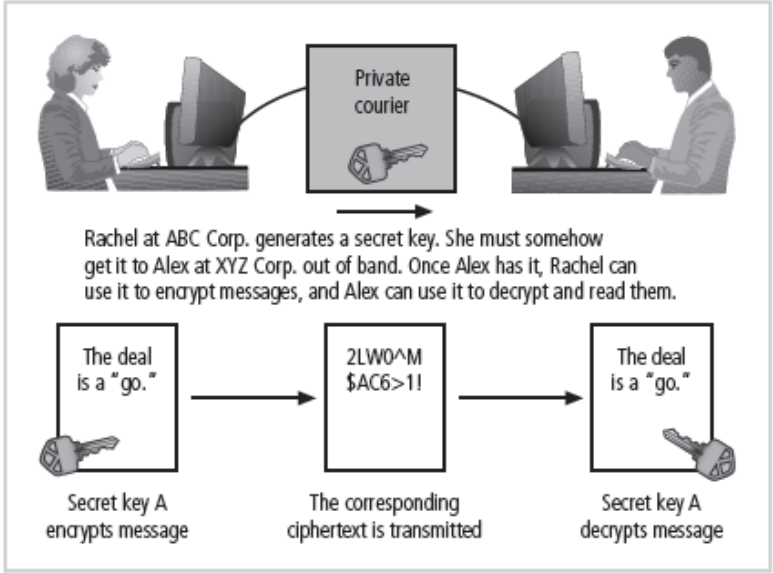

Figure 8-5 Example of Symmetric Encryption

17

Symmetric Encryption (cont'd.)

- 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

18

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

19

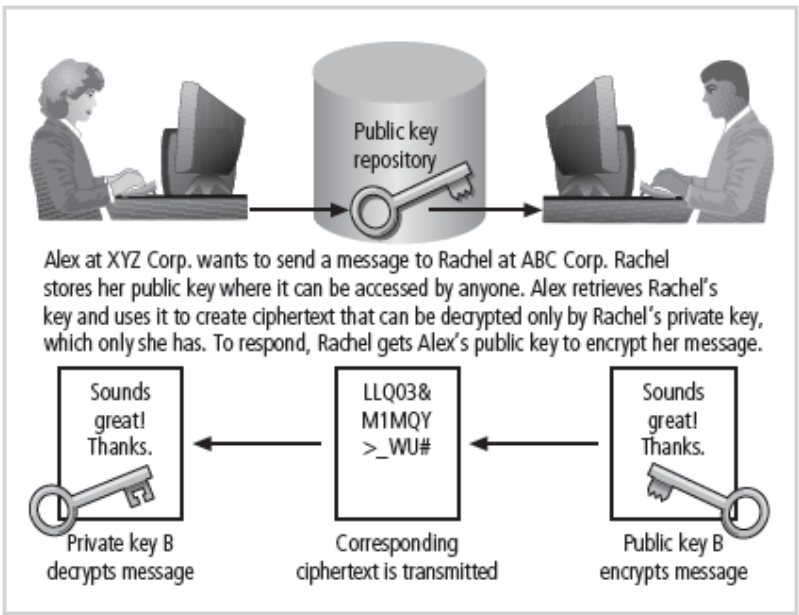

Figure 8-6 Example of Asymmetric Encryption

20

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

21

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

22

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

23

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

24

Digital Signatures

- Created in response to rising need to 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 Signature Standard (DSS)

26

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
- Different client-server applications use different types of digital certificates to accomplish their assigned functions
- Distinguished name (DN): uniquely identifies a certificate entity

27

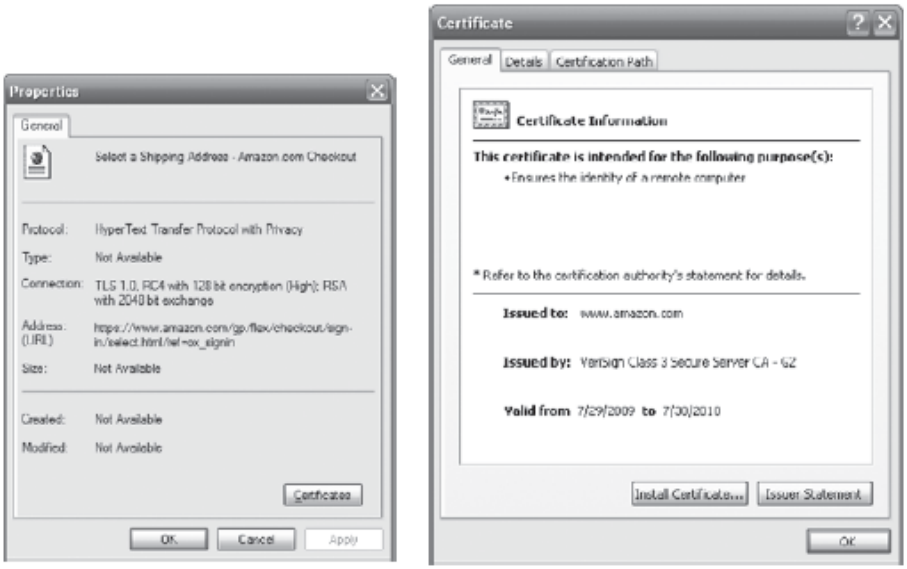

Figure 8-8 Digital Certificate

Version
Certificate Serial Number
Algorithm ID • Algorithm ID • Parameters
Issuer Name
Validity • Not Before • Not After
Subject Name
Subject Public Key Info • 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 8-8 X.509 v3 Certificate Structure[11]

Hybrid Cryptography Systems

- Except with digital certificates, pure asymmetric key encryption not widely used
- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
- Diffie-Hellman Key Exchange method:
  - Most common hybrid system
  - Provided foundation for subsequent developments in public-key encryption

30

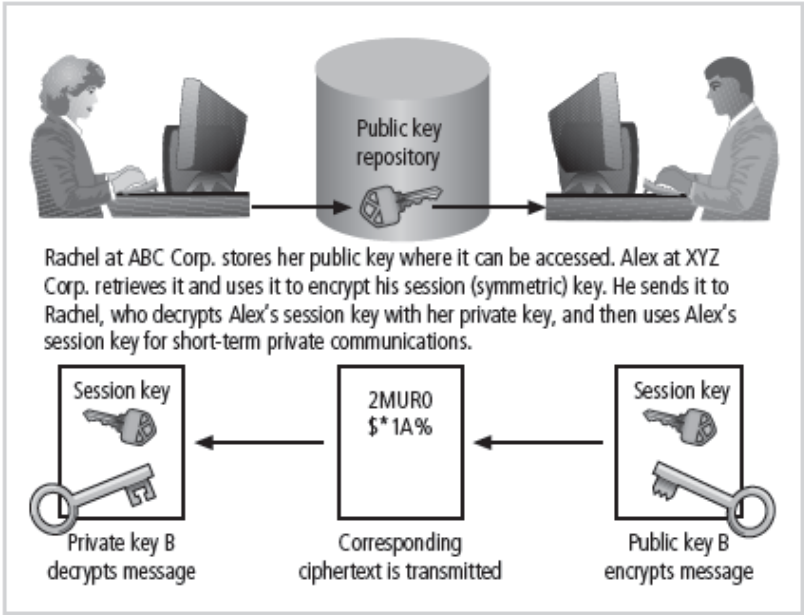

Figure 8-9 Example of Hybrid Encryption

31

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

32

Protocols for Secure Communications

- Much 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

33

Securing Internet Communication with 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
  - Allows encryption of information passing between computers through protected and secure virtual connection

34

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

35

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

36

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP): early attempt to provide security with the 802.11 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
- Bluetooth: can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented

37

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
  - IPSec designed to protect data integrity, user confidentiality, and authenticity at IP packet level
  - IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates
  - In IPSec, IP layer security obtained by use of application header (AH) protocol or encapsulating security payload (ESP) protocol

38

Securing TCP/IP with IPSec and PGP

- 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 guarantees identity
  - Bulk encryption algorithms for encrypting the data
  - Digital certificates signed by a certificate authority to act as digital ID cards

39

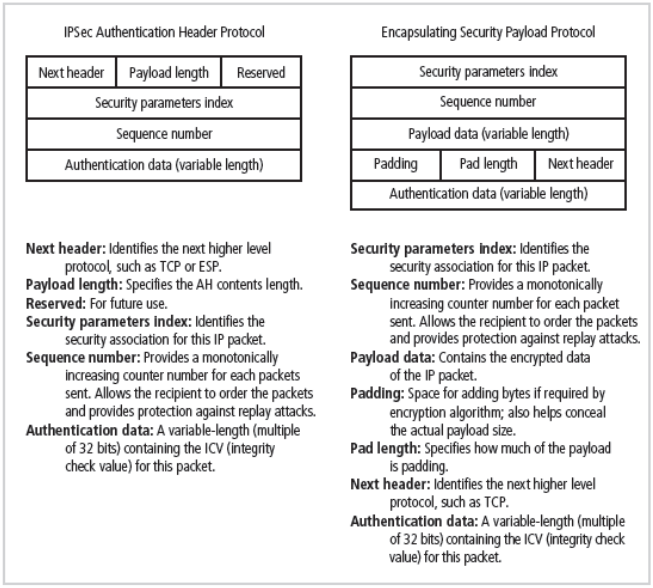

Figure 8-10 IPSec Headers

40

Securing TCP/IP with IPSec and PGP (cont'd.)

- 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

41

Function	Algorithm	Application
Public key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures
Conventional encryption	3DES, RSA, IDEA or CAST	Message encryption
File management	ZIP	Compression

Table 8-12 PGP Functions[24]

42

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

43

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

44

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

45

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)

46

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)

47

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

48

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

49

Summary (cont'd.)

- Strength of encryption tool is dependent on 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
- Cryptosystems are subject to attack in many ways