Cryptography

8

> Yet it may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.
>
> **EDGAR ALLAN POE, THE GOLD BUG**

PRINCIPLES of INFORMATION SECURITY

Second Edition

Introduction

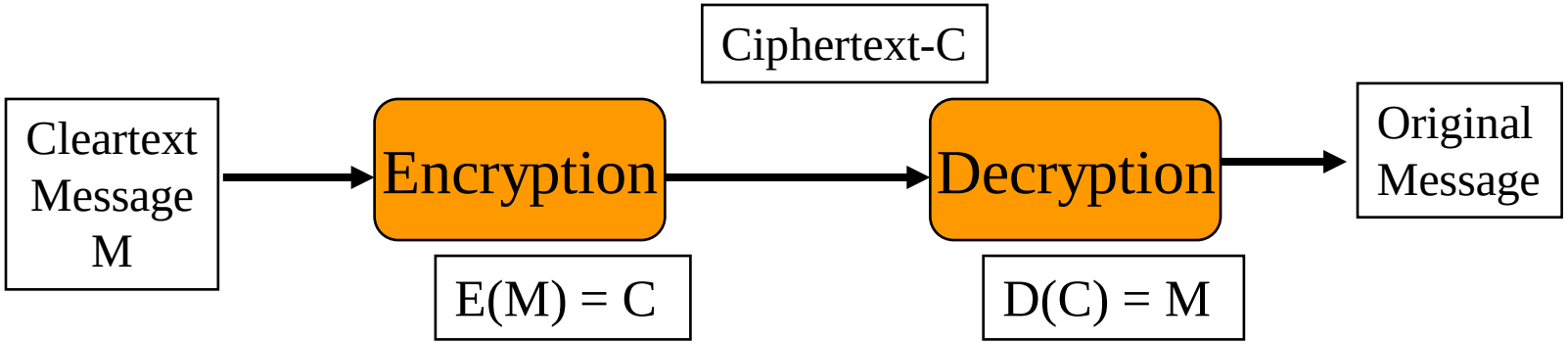
- Although not a specific application or security tool, encryption represents a sophisticated approach to security that is implemented in many security systems.
- In fact, many security-related tools use embedded encryption technologies to protect sensitive information handled by the application.

Principles of Cryptography

- 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

Cipher Methods

- Notations: E(M) = C, D[E(M)]=M, E(M, K) = C
- Plaintext can be encrypted through bit stream or block cipher method



Substitution Cipher

- Each letter in the plaintext is substituted for another letter in C
- This type of substitution is based on a monoalphabetic substitution, since it only uses one alphabet.
- It achieves *confusion* as one of the main technique for obscuring the redundancies in a plaintext message
- *Confusion* obscures the relationship between the plaintext and the ciphertext
- This frustrates attempts to study the ciphertext looking for redundancy and statistical patterns

… Substitution Cipher

- Four types:
  - **A Simple Substitution Ciphers (Monoalphabetic Cipher)**
    - Each character in P is replaced with a corresponding char in C
    - Examples are: Julius Caesar Cipher and ROT13
  - **A Homophonic Substitution Ciphers**
    - Similar to a Simple Substitution Ciphers, but each letter is mapped to more than one letter in C
    - “A” can be mapped to either 5, 13, 26, 55
    - Invented in 1401 and used by German
    - Harder to break than Simple Substitution

… Substitution Cipher

- **A Polygram Substitution Ciphers**
  - Blocks of characters are encrypted in groups
  - "ABA" corresponds to "RTQ" and "THE" to "SIL"
  - Securer than simple Substitution Ciphers
  - Example: The *Playfair* cipher (1854) used by British in WWI
- **A Polyalphabetic Substitution Ciphers**
  - Have multiple one-letter keys, each of which is used to encrypt one letter of the M
  - The 1st key encrypts the 1st letter of the M, the 2nd key encrypts the 2nd letter from the M, and so on
  - After all the keys are used, the keys are recycled

… Substitution Cipher

- Julius Caesar Cipher
  - One of the earliest recorded use of a simple Substitution ciphers
  - Based on Letter shift algorithm
  - Shift Value of 3 {key}
  - Example:
    - a b c d e f g h i j k l m n o p q r
    - 
    - a b c d e f g h i j k l m n o p q r
  - hello => khoor
- ROT13:
  - A simple Substitution ciphers found in UNIX
  - “A” is replaced by “N”, “B” with “O”
  - Encrypting a file twice restores the original file: P = ROT13(ROT13(P))

Vigenère cipher

- Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

TABLE 8-2 The Vigenère Square

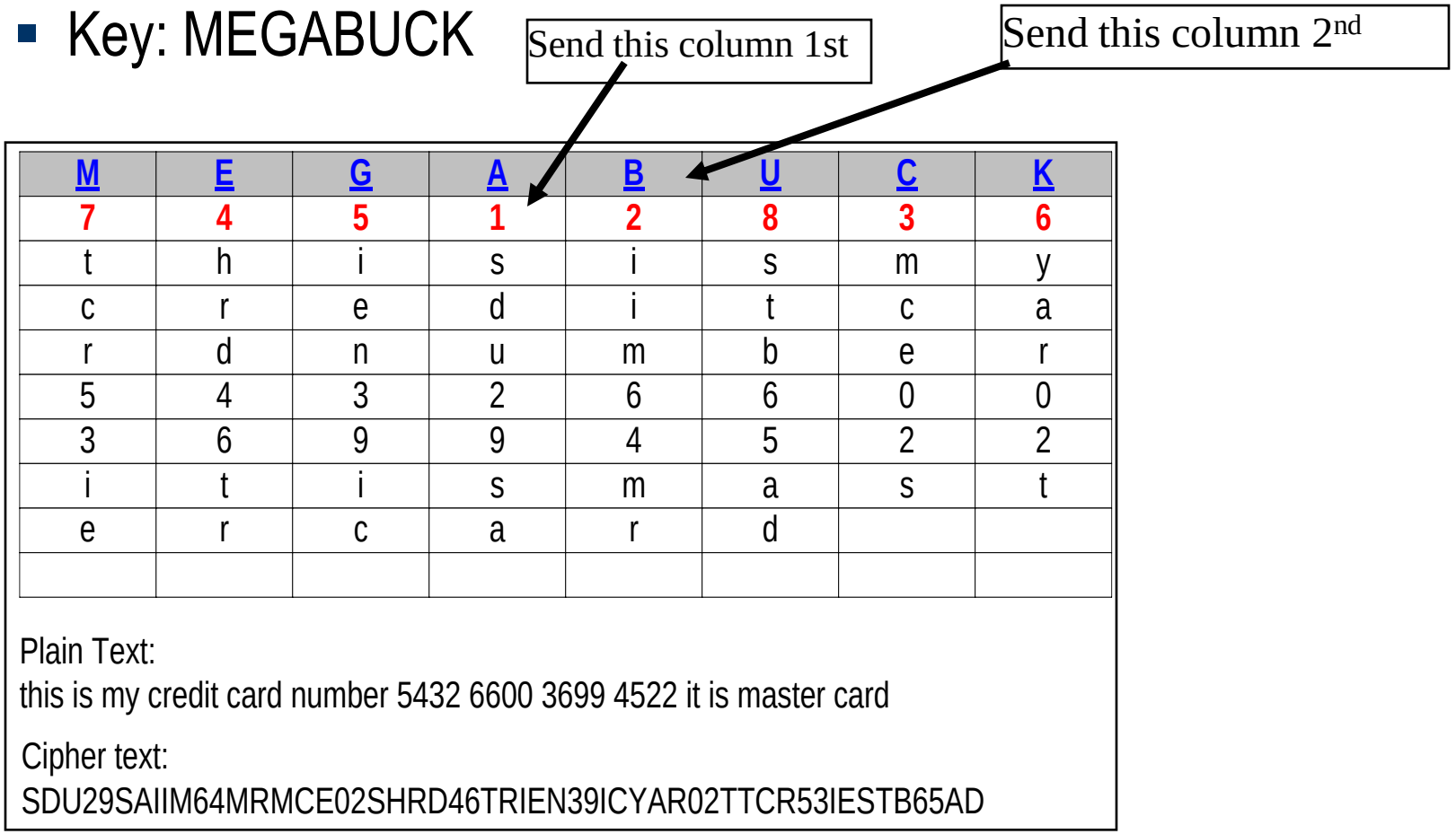
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Transposition Cipher

- The plaintext remains the same but the order of characters is shuffled around
- It achieves *diffusion* as one of the main technique for obscuring the redundancies in a plaintext message
- *Diffusion* dissipates the redundancy of the plaintext by spreading it out over the ciphertext

… Transposition Cipher

- **Column Transposition Ciphers with Key**
  - Key: MEGABUCK



Vernam cipher (One-time Pad)

- Developed at AT&T; uses set of characters once per encryption process
- A perfect encryption scheme (unbreakable using brute force)
- Encrypt (module 26) each letter of the message with a key letter
- The key letter is a large no-repeating set of truly random key letter, written on sheets of paper
- Each key letter is used only once
- M: ONETIMEPAD
- Key: TBFRGFARFM (need a secure channel to pre-shared it)
- Encryption:
  - O + T mod 26 = 15 + 20 mod 26 = 35 mod 26 = 9 = I
  - N + B mod 26 = 14 + 2 mod 26 = 16 mod 26 = 16 = P
- Cipher : IPKLPSFHGQ

Book (running key) cipher

- Uses text in book as key to decrypt a message; ciphertext contains codes representing page, line and word numbers
- A text, typically from a book, is used to provide a very long *key* stream
- Usually, the book to be used would be agreed ahead of time
- Example:
  - Textbook: *The C Programming Language* (1978 edition)
    - Page 63, line 1: *errors can occur in several places. A label has...*
    - **Plaintext***: flee at once*
      Running key*: ERRORSCANO*
      Ciphertext: JCVSRQNPS (f=5, e=4, 5+4 mod 26 = 9 = j); (l=11, r = 17, 11+17 mod 26 = 28 mod 26 = 2 = c)

Symmetric Encryption Examples

- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
  - 64-bit block size; 56-bit key
  - developed in 1977 by IBM and based on the Data Encryption Algorithm (DEA).
  - Adopted by NIST in 1976 as federal standard for encrypting non-classified information
  - DES was cracked in 1997 when Rivest-Shamir-Aldeman (RSA) put a bounty on the algorithm.
  - RSA offered a $10,000 reward for the first person or team to crack the algorithm
  - Fourteen thousand users collaborated over the Internet to finally break the encryption.

Cryptographic Algorithms
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 serves as private key and the other serves as public key
- The public key is stored in a public location, where anyone can use it.
- The private key is a secret known only to the owner of the key pair.
- The problem is that it requires four keys to hold a single conversation between two parties.

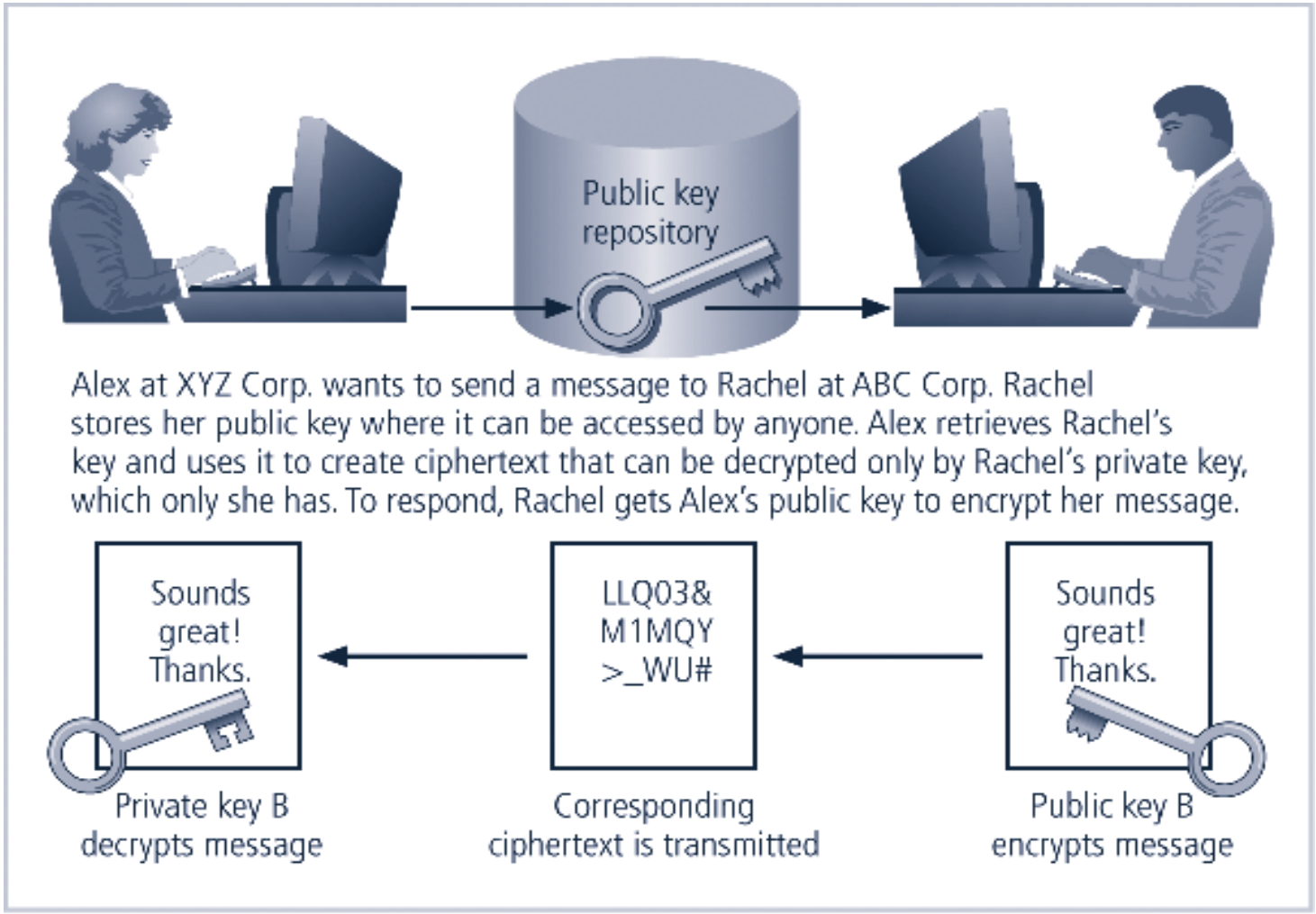


FIGURE 8-4 Example of Asymmetric Encryption

Encryption Key Size

- When using ciphers, size of cryptovariable or key 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

TABLE 8-7 Encryption Key Power

Number of Bits in Key	Odds of Cracking: 1 in	Estimated Time to Crack*
8	256	.000032 seconds
16	65,536	.008192 seconds
24	16,777,216	2.097 seconds
32	4,294,967,296	8 minutes 56.87 seconds
56	72,057,594,037,927,900	285 years 32 weeks 1 day
64	18,446,744,073,709,600,000	8,090,677,225 years
128	3.40282E+38	5,257,322,061,209,440,000,000 years
256	1.15792E+77	2,753,114,795,116,330,000,000,000,000, 000,000,000,000,000,000,000 years
512	1.3408E+154	608,756,305,260,875,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000 years

[NOTE]*Estimated Time to Crack is based on a general-purpose personal computer performing eight million guesses per second.

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)

Cryptography Tools (continued)

- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation

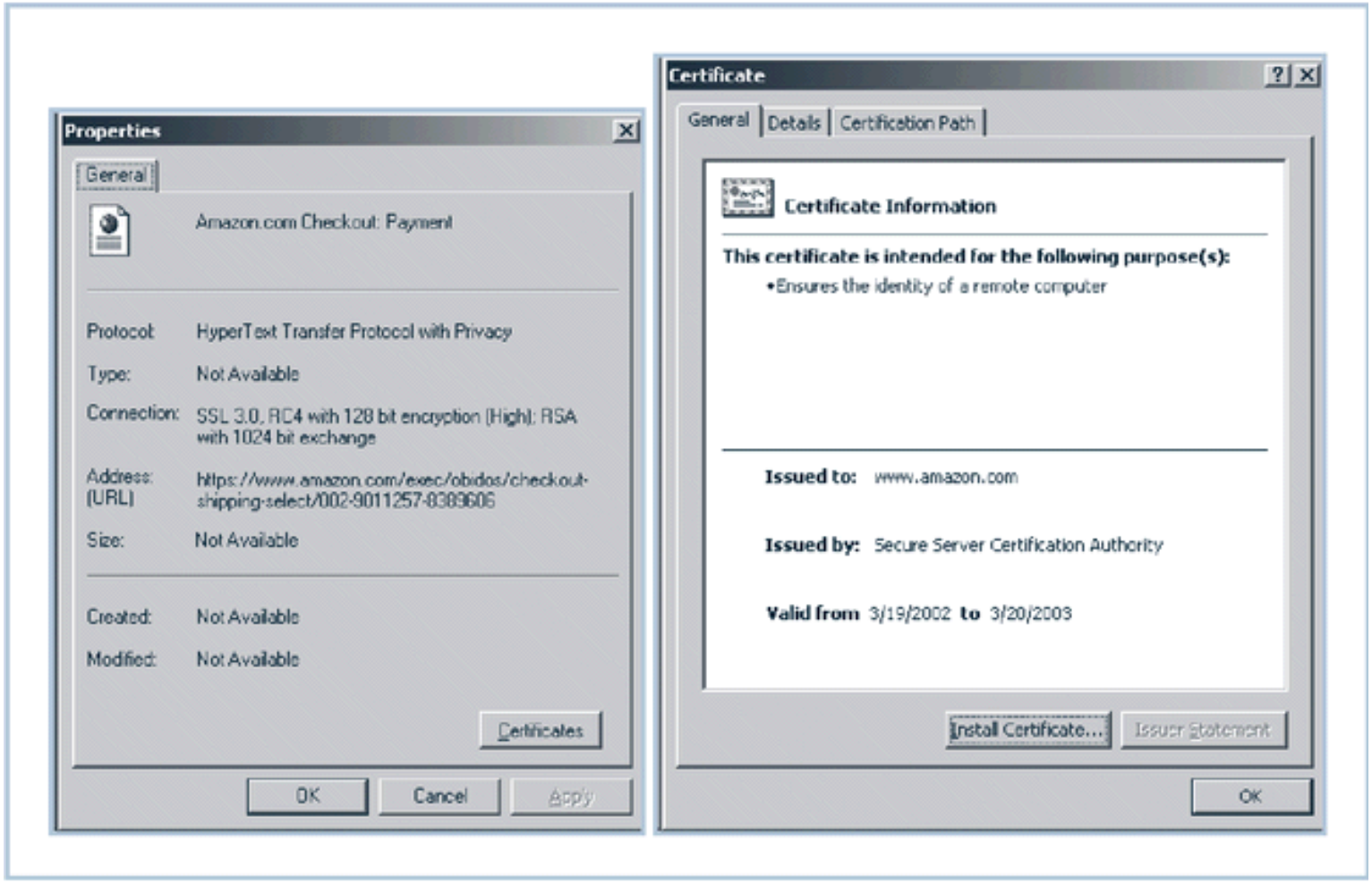
Digital Signatures

- Encrypted messages that can be mathematically proven to be authentic
- The private key is used to encrypt a short message.
- The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be refuted.
- 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
- A Certificate Authority (CA) is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their worth and integrity



Digital Certificates

TABLE 8-8 X.509 v3 Certificate Structure[10]

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

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

Steganography

- Process of hiding information; has been in use for a long time
- The word “steganography” is derived from the Greek words steganos meaning “covered” and graphein meaning “to write.”
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Most computer graphics standards use a combination of three color values (red, blue, and green (RGB)) to represent a picture element, or pixel.
- Each of the three color values usually requires an 8-bit code for that color’s intensity (e.g., 00000000 for no red and 11111111 for maximum red).
- This inability to perceive difference on part of humans provides the steganographer with one bit per color (or three bits per pixel) to use for encoding data into an image file
- 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

- 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 (continued)

- 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 (continued)

- 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

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

Protocols for Secure Communications (continued)

- Securing TCP/IP with PGP
  - 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