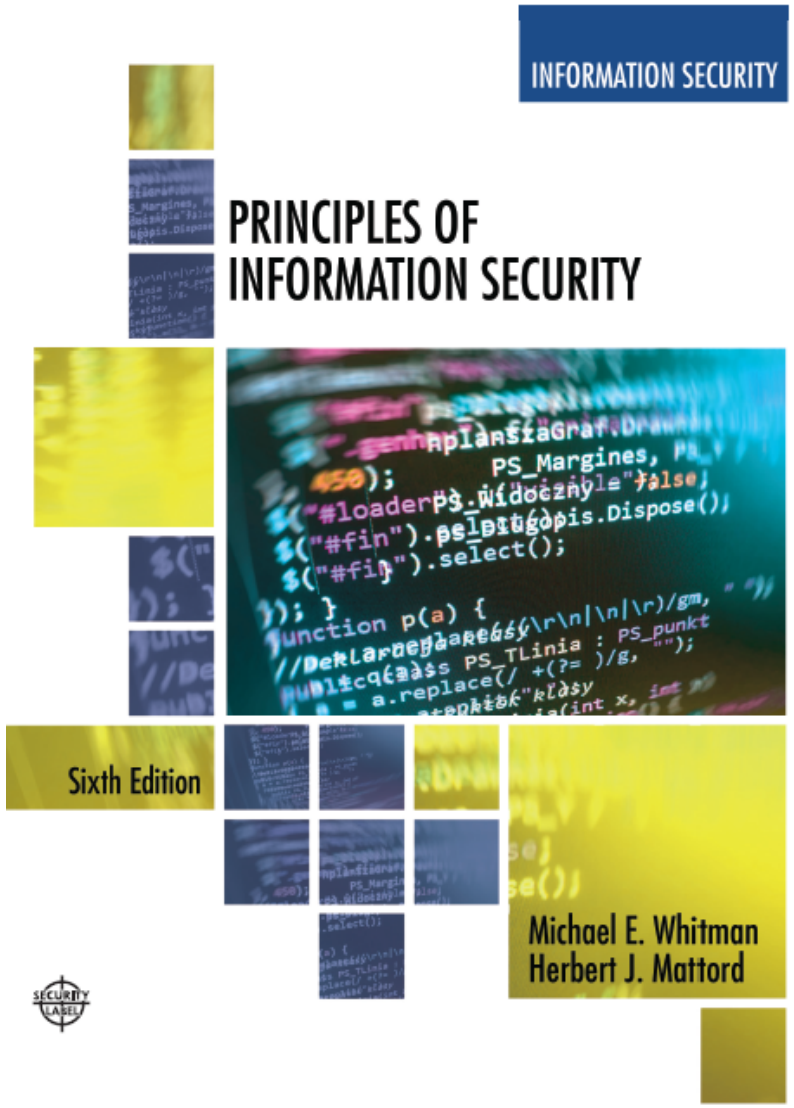


Source: Principles of Information Security

Chapter 8

Cryptography

Dr. Ibrahim Waziri Jr.

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 explain the major protocols used for secure communications

Introduction & Terminologies

Cryptography: the process of making and using codes to secure information.

- 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: each plaintext bit is transformed into a 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 Ciphers

Substitutes cipher exchanges one value for another

- Monoalphabetic substitution
- Polyalphabetic substitution
- Vigenère cipher

	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

- Also known as a permutation cipher; involves simply rearranging the values within a block based on an established pattern.
- 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.

Exclusive OR (XOR)

A function within Boolean algebra used as an encryption function in which two bits are compared.

- If the two bits are identical, the result is a binary 0.
- If the two bits are not identical, the result is a binary 1.

First bit	Second bit	result
0	0	0
0	1	1
1	0	1
1	1	0

Vernam Cipher

- A cryptographic technique developed at AT&T and known as the "one-time pad."
- This cipher uses a set of characters for encryption operations only one time and then discards it.
- 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

Book-Based Ciphers

- Uses text from a predetermined book as a key to decrypt a message.
- Book cipher: ciphertext consists of a list of codes representing page, line, and word numbers of plaintext word.
- Running key cipher: uses a book for passing the 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.

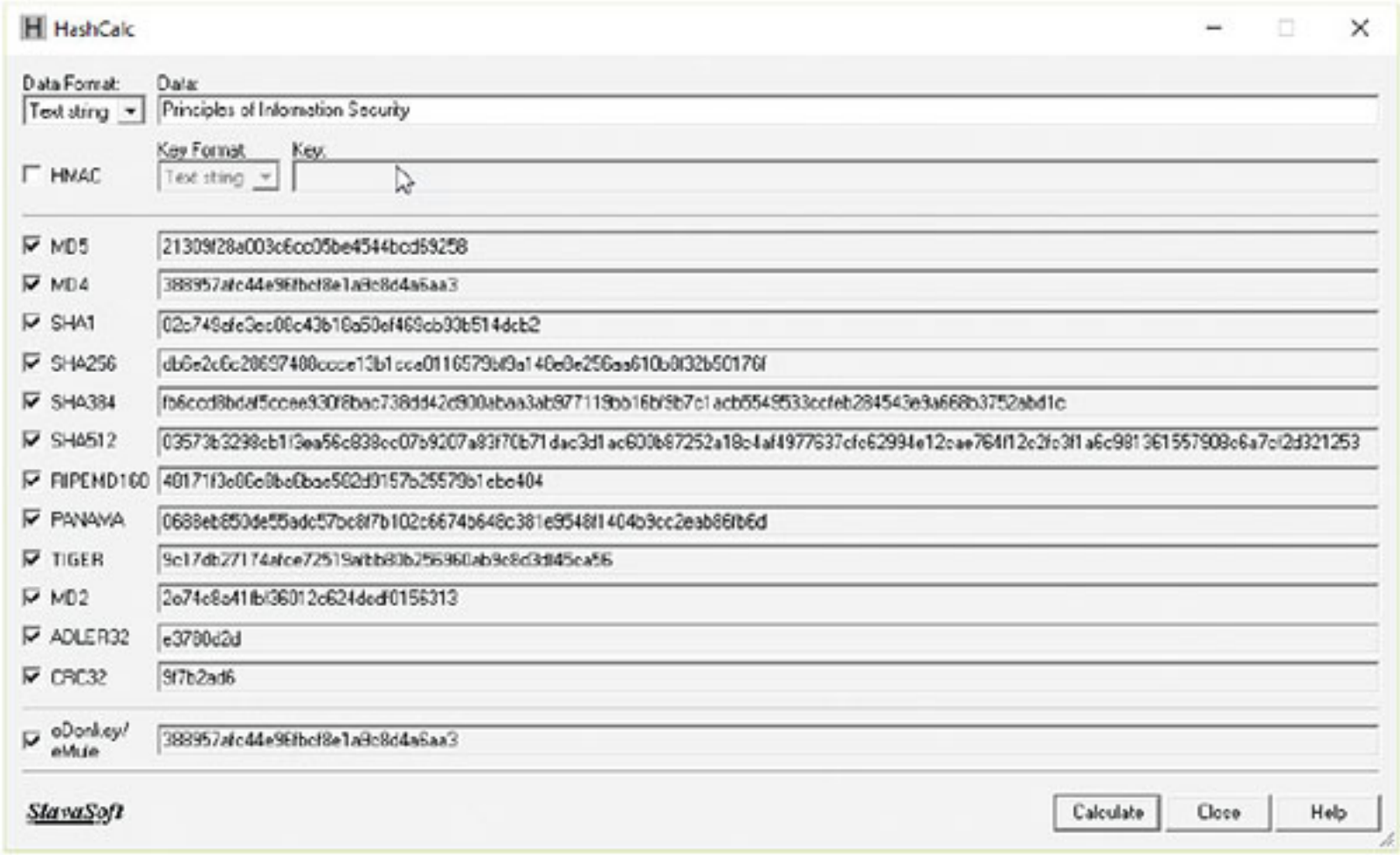
Hash Functions

Mathematical algorithms that create a message summary or digest to confirm message identity and integrity

- Message authentication code (MAC) may be attached to a message

- Used in password verification systems to store passwords and confirm the identity of the user

Hash Functions



Source: SlavaSoft HashCalc.

Cryptographic Algorithms

Today's popular cryptosystems use a combination of both symmetric and asymmetric algorithms.

- Symmetric algorithms.
- Asymmetric algorithms.

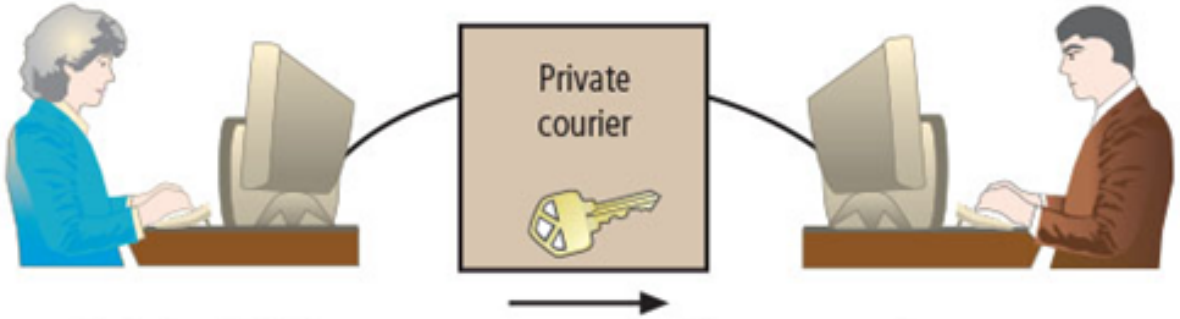
Symmetric Encryption Algorithms

A cryptographic method in which the same algorithm and "secret" are used both to encipher and decipher the message; also known as private-key encryption.

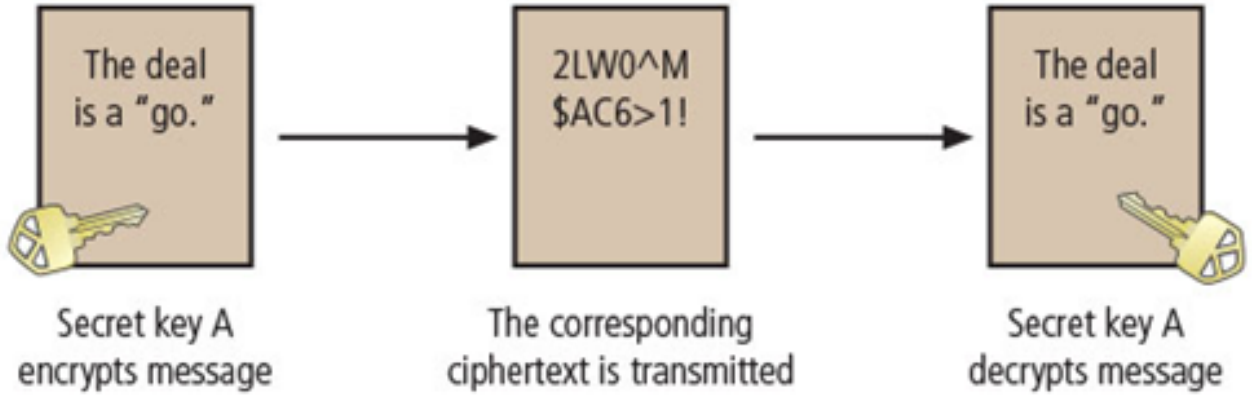
Popular Symmetric Encryption Algorithms:

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)

Symmetric Encryption Algorithms



Rachel at ABC corp. generates a secret key. She must somehow get it to Alex at XYZ corp. out of band. Once Alex has it, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.



Asymmetric Encryption

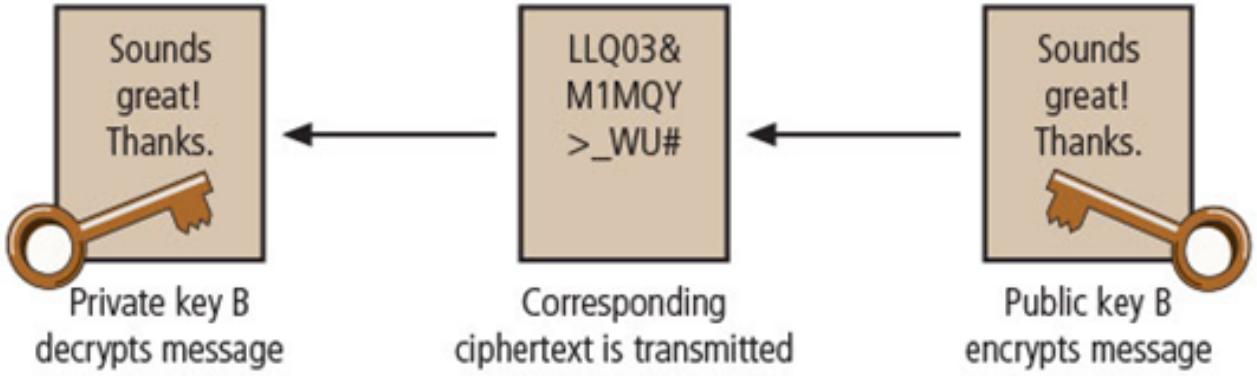
A cryptographic method that incorporates mathematical operations involving two different keys (commonly known as the public key and the private key) to encipher or decipher a message. Also known as public-key encryption.

Popular Asymmetric Encryption:

- RSA (Rivest–Shamir–Adleman)

Asymmetric Encryption

Alex at XYZ corp. wants to send a message to Rachel at ABC corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves Rachel's key and uses it to create ciphertext that can be decrypted only by Rachel's private key, which only she has. To respond, Rachel gets Alex's public key to encrypt her message.



Encryption Key Size

- 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, but on some or all 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 (2k guesses), where k is the number of bits in the key. In reality, the average estimated time to crack is half that time.
- The estimated average time to crack is based on a 2015-era PC with an Intel i7-6700k Quad core CPU performing 207.23 Dhrystone GIPS (billion instructions per second) at 4.0 GHz**

Encryption Key Size

Key Length (Bits)	Maximum Number of Operations (Guesses)	Maximum Time to Crack	Estimated Average Time to Crack
16	65,536	0.0000003 seconds	0.00000016 seconds
24	16,777,216	0.00008 seconds	0.00004 seconds
32	4,294,967,296	0.02 seconds	0.01 seconds
56	7.E+16	4.02 days	2.01 days
64	2.E+19	42.93 years	21.47 years
128	3.E+38	19,005,227,625,557,100, 000,000 years	9,502,613,812,778,540, 000,000 years
256	1.E+77	6,467,143,840,295,770, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	3,233, 571,920,147,890,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years
512	1.E+154	748,844,096, 666,088,000,000,000,000, 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	374,422,048, 333,044,000,000,000,000, 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

Source: www.techspot.com/review/1187-intel-core-i7-6950x-broadwell-e/page4.html.

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

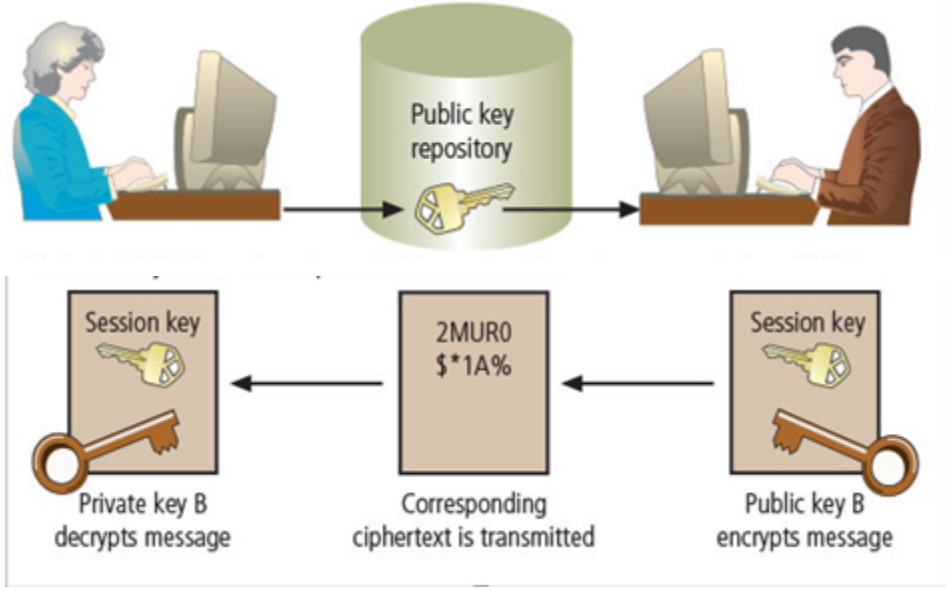
- Public-Key Infrastructure (PKI)
- Digital Signatures
- Digital Certificates

Hybrid Cryptography Systems

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



Rachel at ABC corp. stores her public key where it can be accessed. Alex at XYZ corp. retrieves it and uses it to encrypt his session (symmetric) key. He sends it to Rachel, who decrypts Alex's session key with her private key, and then uses Alex's session key for short-term private communications.

Steganography

The process of hiding messages; for example, hiding a message within the digital encoding of a picture or graphic so that it is almost impossible to detect that the hidden message even exists

- 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

Securing Internet Communication

- Secure Sockets Layer (SSL) & Transport Layer Security (TLS)
- Secure Hypertext Transfer Protocol (S-HTTP)-application of SSL/TLS over HTTP

Securing Email

- Secure Multipurpose Internet Mail Extensions (S/MIME): builds on MIME
- Privacy Enhanced Mail (PEM)
- Pretty Good Privacy (PGP)

Securing Web Transactions (Credit/Debit Cards)

- Secure Electronic Transactions (SET)

Securing Wireless Networks

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA and WPA2)

Securing Remote Connection with VPN

- Internet Protocol Security (IPSec): framework for security development within the TCP/IP family

Summary

- Encryption, Key size, Hash functions, Steganography, Symmetric and Asymmetric.
- The science of encryption, known as cryptology, encompasses cryptography (making and using encryption codes) and cryptanalysis (breaking encryption codes).
- Cryptographic processing methods—bit stream and block ciphering.
- Scrambling data methods--substitution, transposition, XOR, Vigenère & Vernam cipher.
- Public-key infrastructure (PKI)--includes digital certificates and certificate authorities.
- Protocols used for secure communications: S-HTTP, SET, SSL, IPSec, S/MIME, PEM, PGP, WEP, WPA, and WPA2.