



INFORMATION SECURITY

Week 2

Muhammad Taseer ul Islam
taseerulislam@hotmail.com

**Department of Computer Sciences
Federal Urdu University of Arts, Science and
Technology, Islamabad**

X



CRYPTOGRAPHY

2

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

EDGAR ALLAN POE, THE GOLD BUG



KEY TERMS

□ Cryptanalysis

- The process of obtaining the plaintext message from a ciphertext message without knowing the keys used to perform the encryption.

□ Cryptography

- The process of making and using codes to secure information.

□ Cryptology

- The field of science that encompasses cryptography and cryptanalysis



INTRODUCTION

- A variety of cryptographic techniques are used regularly in everyday life.
- For example,
 - a word puzzle that involves unscrambling letters to find a hidden message.
 - Shorthand, or stenography, an abbreviated, symbolic writing method, to take rapid dictation.



INTRODUCTION

- These examples illustrate one important application of cryptography—the efficient and rapid transmittal of information—but cryptography also protects and verifies data transmitted via information systems.



INTRODUCTION

- ❑ The science of encryption, known as **cryptology**, encompasses **cryptography** and **cryptanalysis**.
- ❑ **Cryptography** comes from the Greek words *kryptos*, meaning “hidden,” and *graphein*, meaning “to write,” and involves making and using codes to secure messages.
- ❑ **Cryptanalysis** involves cracking or breaking encrypted messages back into their unencrypted origins.



INTRODUCTION

- ❑ Cryptography uses mathematical algorithms that are usually known to all.
- ❑ After all, it's not the knowledge of the **algorithm** that protects the encrypted message,
- ❑ it's the knowledge of the **key**—a series of characters or bits injected into the algorithm along with the original message to create the encrypted message.



INTRODUCTION

- Background of cryptology
- Key concepts in cryptography
- Common cryptographic tools.
- Common cryptographic protocols
- Some of the attack methods used against cryptosystems.



TERMINOLOGY

- **Algorithm:** The mathematical formula or method used to convert an unencrypted message into an encrypted message. This sometimes refers to the programs that enable the cryptographic processes.
- **Bit stream cipher:** An encryption method that involves converting plaintext to ciphertext one bit at a time.
- **Block cipher:** An encryption method that involves dividing the plaintext into blocks or sets of bits and then converting the plaintext to ciphertext one block at a time.
- **Cipher:** When used as a verb, the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components or vice versa (see *decipher* and *encipher*); when used as a noun, the process of encryption or the algorithm used in encryption, and a term synonymous with *cryptosystem*.

TERMINOLOGY

- **Ciphertext or cryptogram:** The ~~unintelligible encrypted~~ or encoded message resulting from an encryption.
- **Code:** The process of converting components (words or phrases) of an unencrypted message into encrypted components.
- **Decipher:** See *Decryption*.
- **Decryption:** The process of converting an encoded ~~or enciphered~~ message (ciphertext) back to its original readable form (plaintext). Also referred to as *deciphering*.
- **Encipher:** See *Encryption*.
- **Encryption:** The process of converting an original message (plaintext) into a ~~form that cannot be used by unauthorized individuals~~ (ciphertext). Also referred to as *enciphering*.



TERMINOLOGY

- ✓ • **Key or cryptovariable:** The information used in conjunction with the algorithm to create the ciphertext from the plaintext; it can be a series of bits used in a mathematical algorithm or the knowledge of how to manipulate the plaintext. Sometimes called a cryptovariable.
- ✓ • **Keyspace:** The entire range of values that can be used to construct an individual key.
- ✓ • **Link encryption:** A series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then reencrypts the message using different keys and sends it to the next neighbor. This process continues until the message reaches the final destination.

✓ **TERMINOLOGY**

- ✓ • **Plaintext or cleartext:** The original unencrypted message that is encrypted and is the result of successful decryption.
- ✓ • **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.
- ✓ • **Work factor:** The amount of effort (usually expressed in units of time) required to perform cryptanalysis on an encoded message.



CIPHER METHODS

- In the **bit stream method**,
- each bit in the plaintext is transformed into a cipher bit one bit at a time.
- In the **block cipher method**,
- the message is divided into blocks—for example, sets of 8-, 16-, 32-, or 64-bit blocks—and then each block of plaintext bits is transformed into an encrypted block of cipher bits using an algorithm and a key.



CIPHER METHODS

- ❑ **Bit stream methods** commonly use algorithm functions like the exclusive OR operation (XOR),
- ❑ whereas **block methods** can use substitution, transposition, XOR, or some combination of these operations, as described in the following sections.
- ❑ Note that most computer-based encryption methods operate on data at the level of its binary digits (bits), while others operate at the byte or character level.



CIPHER METHODS

▣ Substitution Cipher

▣ Key Terms

- ▣ **Monoalphabetic Substitution** A substitution cipher that only incorporates a single alphabet in the encryption process.
- ▣ **Polyalphabetic Substitution** A substitution cipher that incorporates two or more alphabets in the encryption process.
- ▣ **Substitution Cipher** An encryption method in which one value is substituted for another.
- ▣ **Vigenère Cipher** An advanced type of substitution cipher that uses a simple polyalphabetic code.



CIPHER METHODS

▣ Substitution Cipher

- ▣ A substitution cipher exchanges one value for another
—for example,
it might exchange a letter in the alphabet with the letter three values to the right, or it might substitute one bit for another bit four places to its left.

R ✓

CIPHER METHODS

▣ Substitution Cipher

▣ Initial alphabet:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Yields

▣ Encryption alphabet:

DEFGHIJKLMNOPQRSTUVWXYZABC



CIPHER METHODS

▣ Substitution Cipher

- ▣ The previous example of substitution is based on a single alphabet and thus is known as a **monoalphabetic** substitution.
- ▣ More advanced substitution ciphers use two or more alphabets, and are referred to as **polyalphabetic** substitutions

CIPHER METHODS

▣ Substitution Cipher

- ▣ To extend the previous example, consider the following block of text:

Plaintext:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution cipher 1:	DEFGHIJKLMNOPQRSTUVWXYZABC
Substitution cipher 2:	GHIJKLMNOPQRSTUVWXYZABCDEF
Substitution cipher 3:	JKLMNOPQRSTUVWXYZABCDEFGHI
Substitution cipher 4:	MNOPQRSTUVWXYZABCDEFGHIJKL

TEXT ▣ WKGF



A vibrant neon sign with the words "QUIZ TIME" in a stylized, bubbly font. The word "QUIZ" is rendered in pink neon, while "TIME" is in cyan. The sign is enclosed in a decorative frame made of alternating pink and cyan neon lines. The background is a dark blue brick wall.

QUIZ
TIME

Any Questions?