Head Lines

- Introduction
- Definitions

• Introduction

Communication System: Is to connect nodes such as individuals , computers ,phones , telephones ,..etc , via link mode.(sea figure-1)

Advantages of communications:

- To exchange data, information ,knowledge , expert …
- To reduce the distances between nodes
- To share services like the protection, benefits, succors ,reliefs ,...etc.
- And many other advantages are perspective and impalpable advantages .

Figure-1: simple view of the communication system

To achieve the communication and exchange of information, raised another important goal, that is protection the exchangeable information. Therefore, based on the type of communication system, the various scientific fields have risen to the protection of this information. Today, the modern communication systems are computers networks. These computers are in multiple forms like computers, mobiles, control systems, notebooks, ….

Computers Networks

Definition: A computer network is two or more of authoritative connected computers via a communication channel. Figure-2

Computer networks play a key role in modern society. We define a computer network from two perspectives: physically (hardware) and logically (software and data).

Physically From a physical (hardware) perspective, a computer network is a hardware infrastructure interconnecting end-devices, where end-devices can be in one of the many possible forms such as personal computers, personal digital assistants, smart phones, wireless sensors, wireless actuators (e.g. a Philips Hue lamp) and smart televisions.

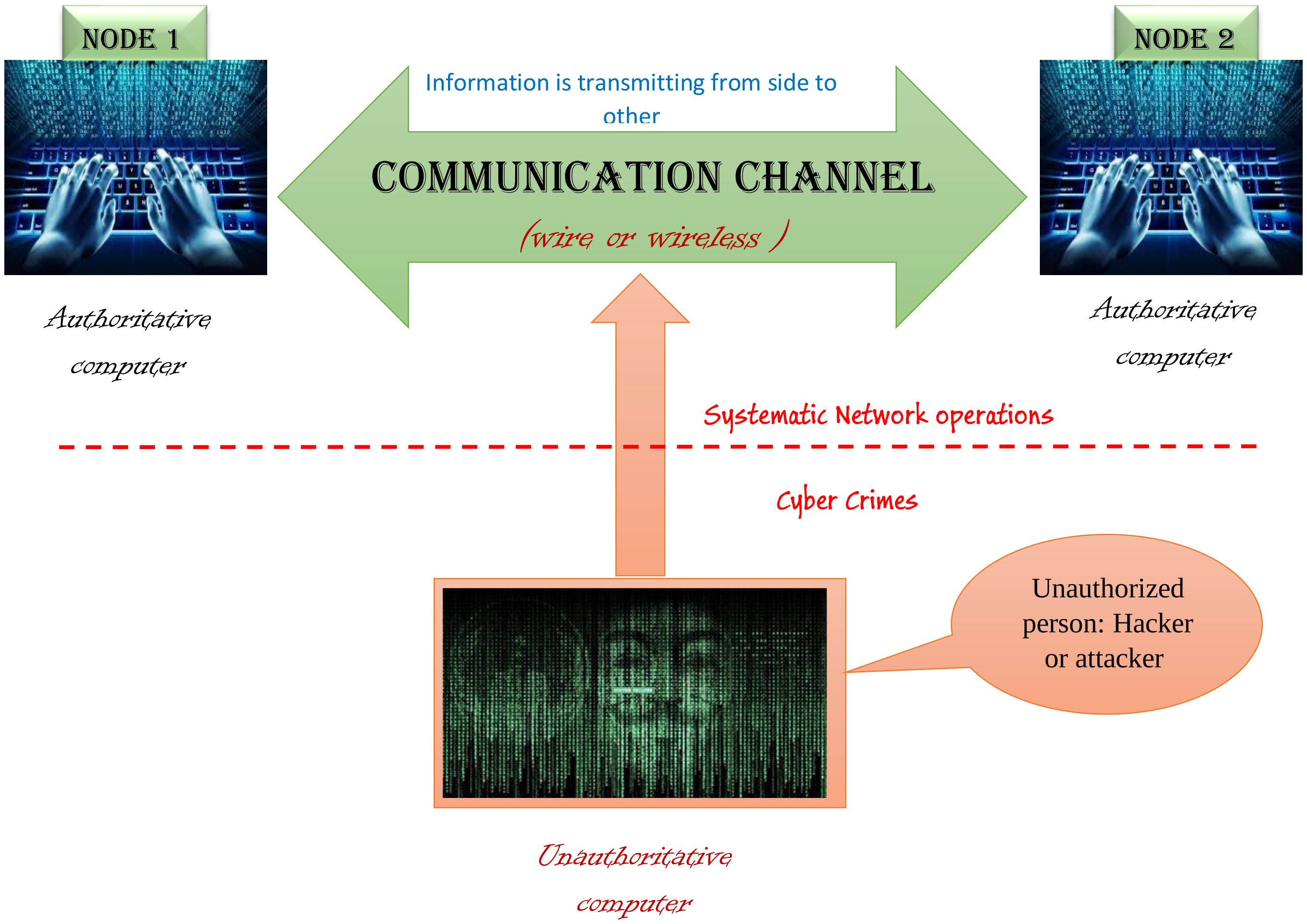

Figure-2: The authorized and unauthorized sides in the computer networks

LOGICALLY From a software and data perspective, a computer network is a system facilitating information exchange between applications that do not share a physical memory component or memory space.

Note: An authorized side in the network, it can be a sender or receiver and it's used, by understanding with others, the suitable technique to protect the exchangeable information from unauthorized side(s). All ***protection secret information techniques***(figure-3) that used they can be either ***disarranging*** the information to transfer it into inapprehensible form, or ***embedding*** the information in a host.

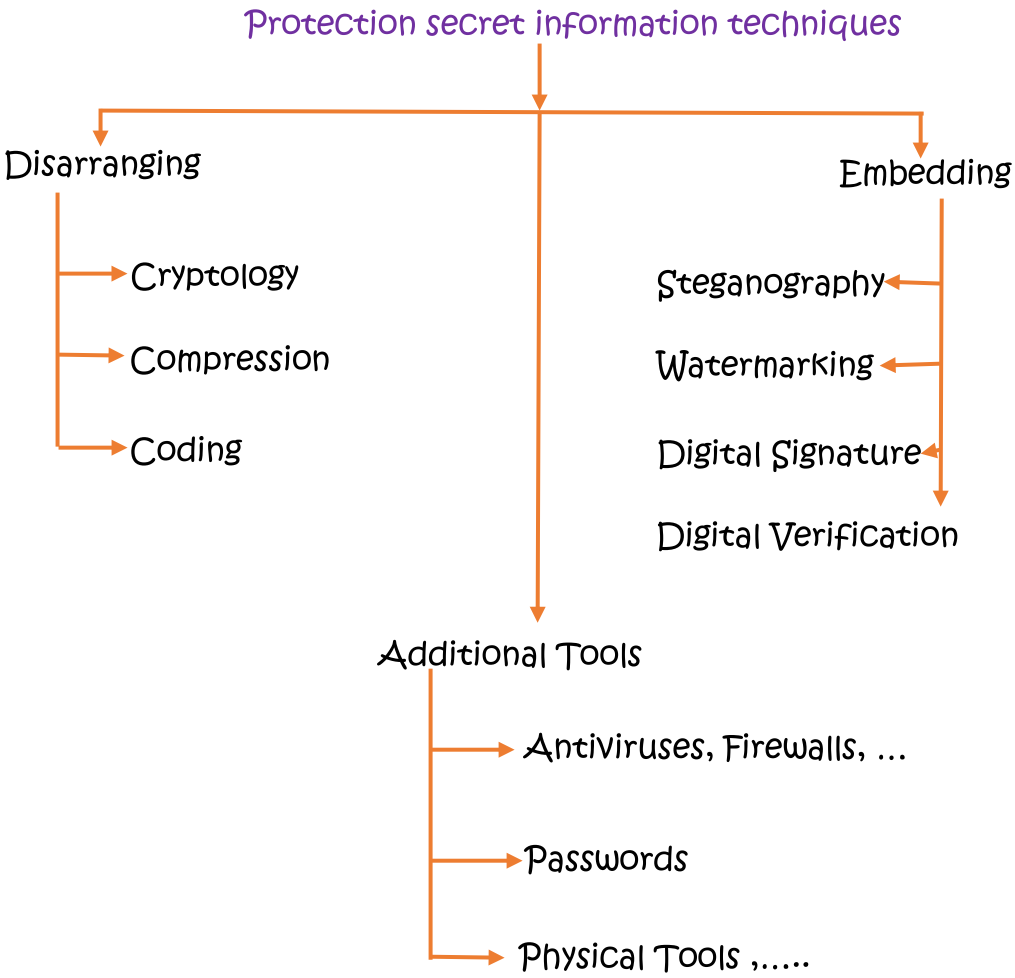

Figure-3: The protection secret information techniques

Definitions

Protection Secret Information Technique: The technique that using to protect a secret information, either it stored in the computer or it exchanged among network via wire or wireless connection.

Cryptology science: A Greek word formed from two syllables, "*crypto*" it means the secret and "*logy*" it means a science. It's the science concerned with data communication and storage in secure and usually secret form. To achieve the goal of data security, it encompasses:

- ***Cryptography***: The word "cryptography" is a Greek word formed from two syllables, the "crypto" it means the secret, and "graphy" it means the writing. The fundamental objective of cryptography is to enable two people, usually referred to as node1 and node2, to communicate over an insecure channel in such a way that an telephone line or computer network, for example. The information that node1wants to send to node2, which we call “plaintext” or " message" can be in any natural language as English text, numerical data, or anything at all — its structure is completely arbitrary. Node1 encrypts the plaintext, using a predetermined key(protocol of cryptosystem) , and sends the resulting ciphertext over the channel. Node3, upon seeing the ciphertext in the channel by eavesdropping, cannot determine what the plaintext was; but node2, who knows the encryption key, can decrypt the ciphertext and mathematical notation. (figure 4)

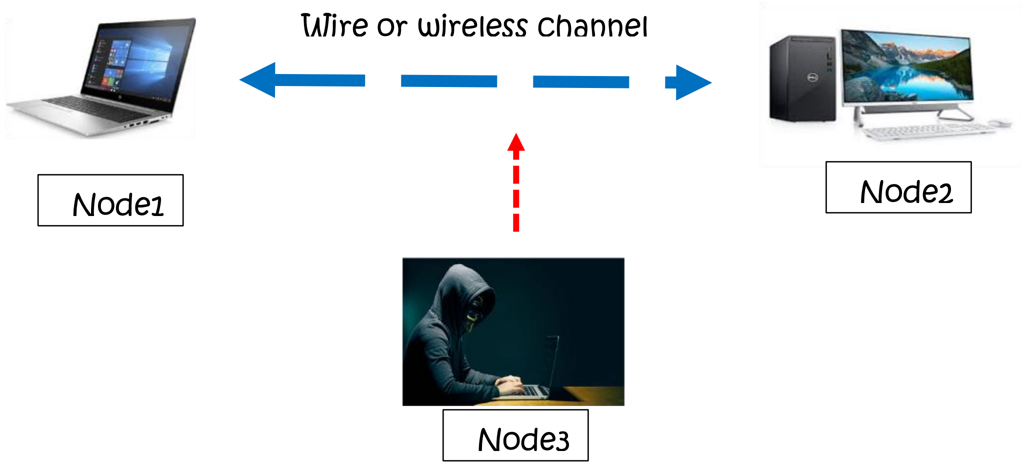

Figure-4: Two nodes network with external computer threat

Definition1: A cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext to encode or decode messages securely. The term “cryptosystem” is shorthand for “cryptographic system” and refers to a computer system that employs cryptography, a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. To help keep data secure, cryptosystems incorporate the algorithms for key generation, encryption and decryption techniques. At the heart of cryptographic operations is a cryptographic key, a string of bits used by a cryptographic algorithm to transform plain text into ciphertext or the reverse. The key is part of the variable data provided as input to a cryptographic algorithm to execute this sort of operation. The cryptographic scheme’s security depends on the security of the keys used. **Cryptosystems are used for sending messages in a secure manner over the internet, such as credit card information and other private data. In another application of cryptography, a system for secure electronic mail.**

Components of cryptosystems

A basic cryptosystem includes the following components:

- Plaintext- This is the data that needs to be protected.(also called a message, and abbreviated P)
- Encryption algorithm- This is the mathematical algorithm that takes plaintext as the input and returns ciphertext. It also produces the unique encryption key for that text.($C= E_{ek}(P)$)
- Ciphertext- This is the encrypted, or unreadable, version of the plaintext.(abbreviated C)
- Decryption algorithm- This is the mathematical algorithm that takes ciphertext as the input and decodes it into plaintext. It also uses the unique decryption key for that text.($P=D_{dk}(C)$)
- Encryption key- This is the value known to the sender that is used to compute the ciphertext for the given plaintext. (abbreviated ek)

- Decryption key- This is the value known to the receiver that is used to decode the given ciphertext into plaintext. (abbreviated dk)

Types of cryptosystems

Cryptosystems are categorized by the method they use to encrypt data, either symmetrically or asymmetrically.

1. *Symmetric key* encryption is when the cryptosystem uses the same key for both encryption and decryption. In this method, keys are shared with both parties prior to transmission and are changed regularly to prevent any system attacks. **(ek=dk)**

2. *Asymmetric key* encryption is when the cryptosystem uses different keys for encryption and decryption. However, the keys are mathematically related. In this method, each party has their own pair of keys that is exchanged during transmission. (ek≠dk)

- ***Cryptanalysis:*** Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown or some time cryptographic encryption algorithm is unknown.
- ***Designing:*** This field concerned with design the cryptographic algorithms.
- ***Evaluation***: The main goal of this branch is evaluating cryptographic algorithms by the search for gaps and breaches and reform.

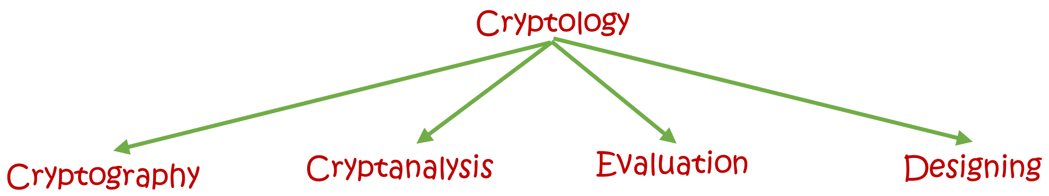

Figure-5: Cryptology branches

To illustrate the concept of cryptography and its components, more likely to give the explanation of a simple cipher, that is Caesar cipher.

a ***Caesar cipher***, also known as a **Caesar's cipher**, the **shift cipher**, **Caesar's Code** or **Caesar Shift**, is one of the simplest and most widely-known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions further down the alphabet(figure-6). For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

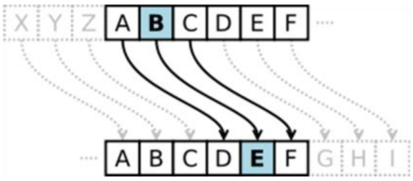

Figure-6: The schema of Caesar cipher

Or Encryption algorithm or schema is :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Encryption key is 3.

Or Decryption Algorithm or schema is :

DEFGHIJKLMNOPQRSTUVWXYZABC

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Decryption key is 3

Example: plain text is CAESARCIPHER

Then the cipher text is FDHVDOF