2.4.2 Cryptography Facts

Cryptography is the science of converting data into a secret code to hide a message's meaning during transmission. Cryptographic systems provide the following security services:

- **Confidentiality** by ensuring that only authorized parties can access data.
- **Integrity** by verifying that data has not been altered in transit.
- **Authentication** by proving the identity of the sender or receiver.
- **Non-repudiation** by validating that communications have come from a particular sender at a particular time.

The following terms are related to cryptography:

Term	Definition
Plaintext	*Plaintext* is the readable form of an encrypted message. The term *plaintext* should not be confused with the term *cleartext*, which is information that will not be encrypted. Plaintext is information that will eventually be input into an encryption algorithm.
Ciphertext	*Ciphertext* is the encrypted form of a message that makes it unreadable to all but those the message is intended for.
Cryptanalysis	*Cryptanalysis* is the method of recovering original data that has been encrypted without having access to the key used in the encryption process. This can be done to measure and validate the strength of a cryptosystem. It can also be done to violate the confidentiality and/or integrity of a cryptosystem.
Key	A *key* is a variable in a cipher used to encrypt or decrypt a message. The key should be kept secret. The *key space* is the range of the possible values that can be used to construct a key. Generally speaking, the longer the key space, the stronger the cryptosystem.
Algorithm	A *cipher* or *algorithm* is the process or formula used to convert a message or otherwise hide its meaning. Examples of algorithms include: ▪ A *transposition cipher* (also called an *anagram*), which changes the position of characters in the plaintext message. ▪ A *substitution cipher*, which replaces one set of characters with symbols or another character set. A *code* substitutes hidden words with unrelated terms. ▪ A *one-time pad* is a cryptography method in which plaintext is converted to binary and combined with a string of randomly generated binary numbers (referred to as the *pad*). It is a form of substitution.
Encryption	*Encryption* is the process of using an algorithm to transform data from plaintext to ciphertext in order to protect the confidentiality, integrity, and authenticity of the message.
Decryption	*Decryption* is the procedure used to convert data from ciphertext into plaintext.
Steganography	*Steganography*, which literally translates to 'concealed writing,' hides data or a message so that only the sender or the recipient suspects that the hidden data exists. With steganography, the message is in cleartext. It is not encrypted, but merely hidden. Examples of steganography include: ▪ Embedding still pictures in a video stream. The picture can only be viewed by stepping through the video frame by frame (playing the video in real time hides the image because the eye cannot see one single frame within the video). ▪ Hiding text messages or hiding alternate images within a photograph. With this method, data is distributed inside the last two bits of each color. When viewed normally, the hidden information cannot be detected. Using special tools, the data in the last two bits of each color is extracted to recreate the original. ▪ With *watermarking*, hidden data is embedded into an image or a file to prove ownership. Because the file contains the special data sequence, a file with that embedded data could only have come from the original source. ▪ *Microdots* are images shrunk down to the size of a period, then included in a seemingly harmless message.