Olatinwo Mubarak

16/SCI01/034

1. Steganography- Steganography (literally meaning *covered writing*) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shaved messenger's head, letting his hair grow back, then shaving it again when he arrived at his contact point. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

1. Steganography vs Cryptography

|  |  |
| --- | --- |
| Steganography | Cryptography |
| Steganography means **cover writing.** | Cryptography means **Secret writing.** |
| Steganography is less popular than Cryptography. | While cryptography is more popular than Steganography. |
| Attack’s name in Steganography is Steganalysis. | While in cryptography, Attack’s name is Cryptanalysis. |
| In steganography, structure of data cannot be altered. | While in cryptography, structure of data can be altered. |
| Steganography supports Confidentiality and Authentication security principles. | While cryptography supports Confidentiality and Authentication security principles as well as Data integrity and Non-repudiation. |
| Steganography relies on parameter such as **Key**. | While cryptography does not rely on any parameter. |

1. Block Cipher- A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. Block ciphers, like Playfair and Hill ciphers, encrypt plaintext of a fixed length – digraphs for the Playfair cipher and n-graphs for n-dimensional Hill ciphers. If the length of the plaintext message is not an integral multiple of the length of a block, the plaintext message must be padded. For example, a common block cipher, AES, encrypts 128-bit blocks with a key of predetermined length: 128, 192, or 256 bits. Block ciphers are pseudorandom permutation (PRP) families that operate on the fixed size block of bits. PRPs are functions that cannot be differentiated from completely random permutations and thus, are considered reliable, until proven unreliable.

Stream Cipher- Stream ciphers can encrypt plaintext messages of variable length. The one-time pad can be thought of as an example – each message uses a portion of the key with length equal to the length of the plaintext message. (Then that portion of the key is never re-eused.)