**ADEYEMI TESLIMAT ADEBUNMI**

**16/SCI01/003**

**CSC 418 ASSIGNMENT**

1. Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.
2. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security.
3. 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. 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. Block cipher modes of operation have been developed to eliminate the chance of encrypting identical blocks of text the same way, the ciphertext formed from the previous encrypted block is applied to the next block. A block of bits called an initialization vector (IV) is also used by modes of operation to ensure ciphertexts remain distinct even when the same plaintext message is encrypted a number of times. Some of the various modes of operation for block ciphers include CBC (cipher block chaining), CFB (cipher feedback), CTR (counter), and GCM (Galois/Counter Mode), among others. Above is an example of CBC mode.

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.) The ideas that resulted in modern stream ciphers originated with another AT&T Bell Labs engineer, Gilbert Vernam (1890 – 1960). In 1917, Vernam developed a scheme to encrypt teletype transmissions. Unlike Morse code, which uses symbols of different lengths to substitute for letters of the alphabet, teletype transmission used what we would today call a 5-bit code for the letters of the alphabet and certain keyboard commands. Its use was similar to the way that the 8-bit ASCII code is used today in computing. A = xxiii B = x••xx C = ixxxi D = x E = x i i ii i x iiii F = x xi x G = H = i i x xx ii i x x I = i i xx J = xxi i x K = xxxxi L = i ii x x M = iixxx N = ii i xx O = iiixx P = i i xx x Q = xxxix R = iii x x S = x xi ii T = iiiix U = xxxii V = ixxxx W = xxiix X = x xi xx Y = xi i x x Z = xiiix