NAME: OKEKE OTITOCHI MARYANN

MAT NO:16/SCI01/030

1. **Steganography** is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from New Latin steganographia, which combines the Greek words steganós, meaning "covered or concealed", and -graphia meaning "writing". 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.

2. DIFFRENCES BETWEEN STEGANOGRAPHY AND CYPTOGRAPHY

BASIC	It is known as cover writing	It means secret writing
GOAL SECRET	Communication	Data Protection
STRUCTURE OF THE MESSAGE	Not Altered	Altered only of the transmission
POPULARITY	Less popular	More Commonly Used
RELIES ON	Key	No Parameters
TYPES OF ATTACK	Steganalysis	Cryptanalysis
SUPPORTED SECURITY PRINCIPLES	Confidentiality and authentication	Confidentiality, data integrity, authentication, and non-repudiation.
TECHNIQUES	Spacial domain, transform domain, model-based and ad-hoc.	Transposition, substitution, stream cipher, block ciphers.
IMPLEMENTED ON	Audio, Video, image, texts	Only Texts files.

3. 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. 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 cipher text 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 cipher texts 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 modes.

Example of block cipher

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data

4. STREAM CIPHER

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (key stream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the cipher text stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation is an exclusive -or (XOR).

Example of a stream cipher:

RC4 is an example of a modern symmetric-key stream cipher. It was developed in 1987 by Ron Rivest, one of the developers of the public-key cipher RSA. RC4 is a trademark. RC2, RC5, and RC6 are symmetric-key block ciphers.