**NAME: DABO LAURA I.**

**MATRIC NUMBER: 16/SCI01/053.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: CRYPTOGRAPHY.**

**START DATE: 07-05-2020.**

**END DATE: 22-05-2020.**

**QUESTION**

1. What is steganography?
2. Compare and contrast Cryptography and Steganography
3. Discuss block cipher and stream cipher with a given examples.

**ANSWERS**

1. Steganography means cover writing. Steganography is a method of hiding the communication by concealing the secret message is converted into fake message. The main idea behind the steganography is to prevent the suspicion about the existence of the information.
2. Cryptography is the process of hiding secret or private text in an unintelligible for such that a normal person is unable to read the information or text. This is done through various ciphers e.g. playfair, ceaser etc. Here, text remains text and is clearly visible to everyone but in an unintelligible form. Whereas steganography is the process of hiding secret text or private information in an image, audio, video. This is done through steganography tool which are also available online. Here text is hidden in any of the form and only image, audio or video is visible to people.
3. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.
4. Cryptography means secret writing whereas steganography means cover writing.
5. In cryptography, attack’s name is cryptanalysis whereas in steganography, attack’s name in is steganalysis.
6. In cryptography, structure of data can be altered whereas in steganography, structure of data cannot be altered.
7. Cryptography supports confidentiality and authentication security principles as well as data integrity and non-repudiation. While steganography supports confidentiality and authentication security principles.
8. Cryptography does not rely on any parameter. While steganography relies on parameter such as key.
9. Cryptography is implemented on text files only whereas in steganography, implementation is on audio, video, image and text.
10. In cryptography, one can tell that a message has been encrypted, but he cannot decode the message without knowing the proper key. Whereas in steganography, the message itself may not be difficult to decode, but most people would not detect the presence of the message.
11. Block cipher: A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed length block of plaintext which is treated as a whole and used to produce a ciphertext (encrypted text) block of equal length. Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key. A block cipher is a type of cipher that encrypts text by running blocks of the text through an algorithm that jumbles it up. It processes the input and block of elements at a time, producing output block for each input block. The fixed length is called the block size and a typical block size is 64 or 128 bits is used. So for example, a 64-bit block cipher will take in 64 bits of plaintext and encrypt it into 64 bits of ciphertext. In cases where bits of plaintext is shorter than the block size, padding schemes are called into play. Majority of the symmetric ciphers used today are actually block ciphers. DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group.

Stream cipher: A stream cipher is a type of symmetric encryption algorithm that encrypts a digital data stream one bit or one byte at a time instead of using blocks. A stream cipher generates what is called a keystream (a sequence of bits used as a key). It processes the input elements continuously, producing output element one at a time, as it goes along. For example, Vigenere cipher and the Vernam cipher. For a stream cipher implementation to remain secure its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the one-time pad.

For instance, a block cipher would work by encrypting the first paragraph of a book before moving on to the next paragraph. A block cipher would repeat this process until the entire book was encrypted. A stream cipher would start by encrypting the first character of the first paragraph before moving on the next character in the same paragraph. This process is repeated until the entire book is encrypted. Text that has been encrypted by a cipher is called ciphertext. In order to return the ciphertext back to its original state, it must be run through the cipher once again.