CS C 418

Assignment 2 question

What is steganography?

 2. Compare and contrast Cryptography and Steganography

3.Discuss block cipher and stream cipher with a given examples.

Answers

1. Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

|  |  |
| --- | --- |
|  |  |
| 1. | Steganography means cover writing. | Cryptography means Secret writing. |
| 2. | Steganography is less popular than Cryptography. | cryptography is more popular than Steganography. |
| 3. | Attack’s name in Steganography is Steganalysis. | cryptography, Attack’s name is Cryptanalysis. |
| 4. | In steganography, structure of data can not be altered. | cryptography, structure of data can be altered. |
| 5. | Steganography supports Confidentialityand Authenticationsecurity principles. | cryptography supports Confidentialityand Authenticationsecurity principles as well as Data integrity and Non-repudiation. |

2. Comparison between cryptography and steganography

* 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.
* Stream Cipher typically encrypts one byte of the message at that moment instead of using blocks. Let’s take an  example, suppose the original message (plain text) is “blue sky” in ASCII (i.e. text format). When you convert these ASCII into equivalent binary values, it will give the output in 0’s and 1’s form.