PART E: Encryption Theory & Coding Theory

Encryption theory: is one of the important applications of the information theory, which also represents one of the branches of Mathematics and Computer Science , that deals with handling errors during data transfer via the noise channel and that it is possible for many mistakes be corrected. This theory also deals with the characteristics of code and suitability for specific applications.

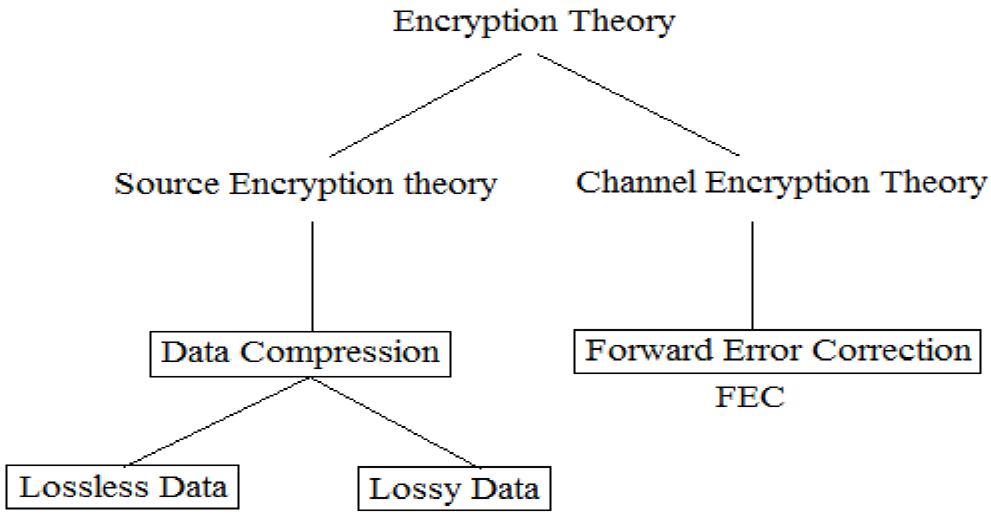

Chart showing encryption systems

Encryption theory consists of:

- ❖ **Channel Encryption Theory:** The aim of the Channel Encryption Theory is to find an encryption can move quickly, these encryptions are legal, and can correct the mistakes that you discover.
  - ○ **<u>Forward Error Correction (FEC)</u>**

    Is the control system for error, which is used to control data transmitted to a system where the sender adds additional data (redundancy) to messages, which allows the recipient to discover the error without the need to ask the sender what the additional data that was added. The benefit of this system (FEC) is to avoid the re-transfer data because the re-transport is relatively expensive and impossible in some cases.

    How FEC system works?

    The FEC system works by adding extra bits for information sent, using a predetermined algorithm so that every extra bit represents a constant function for the original information bits. The original information after that, perhaps appear or not appear in the output encrypted. The code in which the input without any modification in the output, called Systematic while that is not called non-systematic.

Clarifying the principle of FEC

The principle work of FEC way depends on the recipient gives the correct output depending on the most frequent symbol. To make it clear, take the following example:

0 0 0	0
0 0 1	0
0 1 0	0
0 1 1	1
1 0 0	0
1 1 1	1
1 0 1	1
1 1 0	1

Types of FEC

1. **Block Coding**: It works on ***(fixed size block)*** that are symbols or bits are of a predetermined size, and there are kinds of them, but the most common is Reed-Solomon Coding, due to an increase of using on the DVD & Hard Drive. Hamming Distance Algorithm (HD) is considered as an example of this type.
2. **Conventional Coding**: It works on stream of symbols or bits of random length. This is considered as the most commonly used type. Viterbi Algorithm an example of this type.

❖ **Source Encryption Theory (Data Compression):** Source encryption works on the source data compression, in order to ensure that it would send better. This process occurs daily on the internet through the use of compressed files of type ZIP which are used to reduce the load on the Internet and make the files smaller in size. The aim of the *Source Encryption theory* is to save space less storage. When studying the data compression comes to mind the following questions:

- ***What is the Data Compression:*** In computer science and information theory, data compression (source coding) is the process of encoding information using the least number of bits. Data compression works during the connection process, when each of the sender and the recipient understanding the encoding method, also locates on the recipient decompressing the data compression. Data compression is useful because it reduces the consumption of the source, such as the Hard Disk and bandwidth of the channel which defines the data transfer standard.

- ***Why use Data Compression:*** There is a need for data compression for several reasons, the most important of which provide storage space occupied by large-sized files that will allowing to store more files. But in the world of networks and the Internet, the issue is seen as a different way, in terms of dealing with large files such as audio files, video files and other large text.

  All of these files if sent in normal size without compress, it will cause a bottleneck in the traffic through the communications network, and at the same time it will much less data transfer because the time of sending a single file will be great.

  So, they are looking for other ways to allow only for the important data and information to transfer from the file, with the possibility of retrieving the file completely and correctly and without an error occurs.

  For example if there is a file consist of 1000 of A character. We want to send it across a connection network there are more than one choice: first one is to be fully sent, that's mean the file is send as it is. Another solution is to send the letter and next to it number representing the number of times to repeat. This means that we will send one letter and one number next to it. On the receiving side will get the entire file, but at a lower cost.

- ***What types of Data Compression:*** There are two types of data compression, to each of them has the method and the algorithms and the areas of use. There are two types of data compression: Lossless Data Compression and lossy data compression.