Brief Introduction to Cryptography

Cryptography is the art and science of keeping messages secure. When we say "messages" we could be referring to plain text files as well as any other types of files such as executable files. Basically, the point of cryptography is to allow any user to keep his data secure and not readable from not desired individuals.

Before we examine how it works we need to be familiar with certain terms. In order to fully understand some cryptography-related terms, we are going to use the following example. Imagine that you were to send an attached text file by email to your boss. Suppose that the information you are sending him is quite sensitive and it is extremely important to you that only your boss gets to read the message. So, what you do is that you get the text file where that information is. This text file at this point is readable and therefore unsecured. In cryptography we call this the **plaintext** file. So now you need to make the plaintext file unreadable. This is called **encrypting** the data and the result is the **ciphertext** file (encrypted file). The cyphertext file cannot be read and it looks as a sequence of non-sense characters. Only if you decrypt the file you will be able to read it. After you email the cyphertext file to you boss then he would **decrypt** it, which means that he would convert it back to its plaintext form so he could read it. The following diagram (Figure 1) illustrates the encryption/decryption process.

Preview from Notesale.co.uk
Page 2 of 5

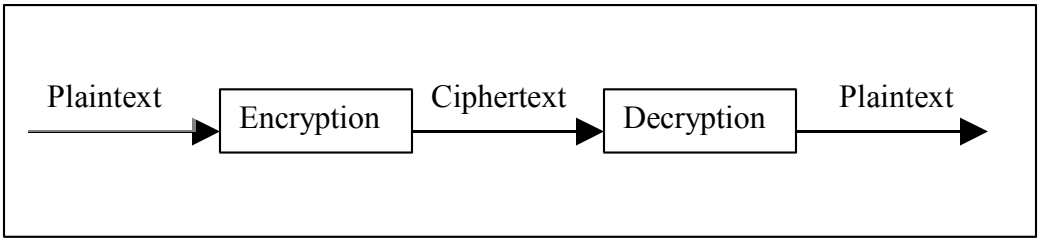

Figure 1