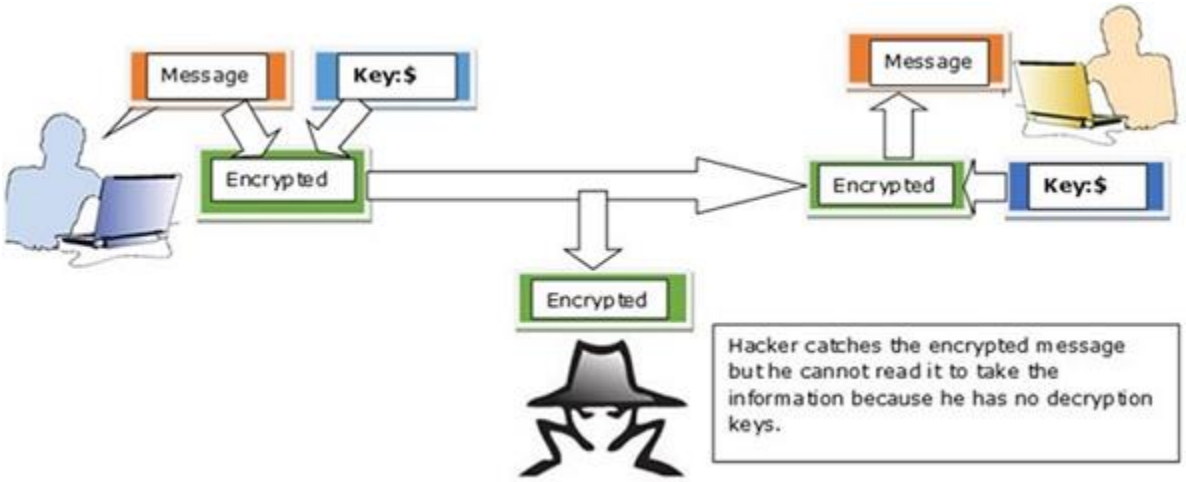
Computer Security - Encryption

In this chapter, we will discuss about the how important Encryption is for Computer Security.

What is Encryption?

Encryption is a transformed type of genuine information where only the authorized parties know how to read it, so in the worst case scenario if somebody has access to these files they would still not be able to understand the message in it.

The bases of encryption are since the ancient times. A good example is the pigeon couriers, where the kings used to send messages to their commandants in the battle field in a specific code, when the enemies caught them, they could not read them, just that the message was lost, but if arrived at the destination commandant had the decryption vocabulary so they could decrypt it.



We should mention that encryption is for good or bad purpose. The bad case is the scenario in which most of the malware files are in an encrypted form, so it cannot be read by everyone accept the hacker.

Tools Used to Encrypt Documents

In this tutorial we will focus more on the practices than on the theoretical aspects for better understanding. Let us discuss about some tools that we use to encrypt documents −

- **Axcrypt** − It is one of the best opensource encryption file softwares. It can be used in Windows OS, Mac OS and Linux as well. This software can be downloaded from − http://www.axantum.com/AxCrypt/Downloads.aspx
- **GnuPG** − This is an opensource software again and it can be integrated with other softwares too (like email). It can be downloaded from − https://www.gnupg.org/download/index.html
- **Windows BitLocker** − It is a Windows integrated tool and its main functions is to secure and encrypt all the hard disk volumes.
- **FileVault** − It is a Mac OS integrated tool and it secures as well as encrypts all the hard disk volume.

Encryption Ways of Communication

System Administrators should use and offer to their staff a secure and encrypted channels of communication and one of them is **SSL (Secure Sockets Layer)**.This protocol helps to establish a secure and encrypted connection between the clients and the servers. Generally, it is used for **Web Servers, Mail Servers, FTP servers**.

Why do you need this?

If you have an online shop and your clients are using their credit card and their personal data to purchase products from it. But they (Data) are at the risk to be stolen by a simple wiretapping as the communication is in clear text, to prevent this, SSL Protocol will help to encrypt this communication.

How to see if the communication is secure?

Browsers give visual cues, such as a lock icon or a green bar, to help visitors know when their connection is secured. An example is shown in the following screenshot.

Another tool used by the system administrator is the **SSH (Secure Shell)**. This is a secure replacement for the telnet and other unencrypted utilities like **rlogin, rcp, rsh**.

It provides a secure channel encrypted in the communication host to host over internet. It reduces the man-in-the-middle attacks. It can be downloaded from – http://www.putty.org/