.Introduction to Cryptography for Non-Technical Personnel, Part 1

.What is Cryptography?

Cryptography is a process or procedure for making some collection of information difficult or impossible to understand. The “collection of information” is often simply a “collection of words”. You can think of the process of “making information, difficult or impossible to understand” as *scrambling*. In cryptography this is formally referred to as *encryption*.

Cryptography is also the process or procedure for taking the scrambled information and returning it to its understandable state. In cryptography this is formally referred-to as *decryption*.

The actual step-by-step process or procedure for scrambling is referred-to as the *cipher*.
The actual step-by-step process or procedure for returning the scrambled information to its understandable state is referred-to as applying the *cipher in reverse*.

Here is a simple example of encryption. You wish to communicate with someone and let him/her know where to meet you. You feel that this meeting place and time needs to be kept private from anyone except the person with whom you are meeting. The message or “collection of words” (as we referred-to above) is:

Meet me four blocks south of the city square, today at noon.

The cipher you will use is to take each letter in the above message and replace it with the next letter of the alphabet. The message, as scrambled, is:

Nffu nf gpvs cmpdlt tpvui pg uif djuz trvbsf, upebz bu oppo.

This (above) approach to encryption is one of two basic approaches, and is called *substitution*. The other basic approach is called *transposition*.

.Why And When Is Cryptography Needed?

Many authors have written lengthy papers on this question. The answers to the question include business needs, national security requirements, societal mores and philosophy. A very short list is included here as a path to a discussion of specific encryption techniques.

1] Confidential information may be left in an accessible place, such as a person’s desktop in a common work area. If the information that was left there had first been encrypted and was viewed by an unauthorized person, it would not be understandable. The actual information, the understandable content, would be safe and secure.

2] In a way similar to #1 (above), information left on the hard disk of a PC could be accessed by an unauthorized person. Even PC operating systems that have a required logon with password can be cracked without too much difficulty. Software programs that automate the cracking of the logon of various PC operating systems are available free on the Internet. The inherent security of logon for a typical PC operating system is many, many orders of magnitude weaker than the security offered by a file encryption program such as KetuFile. Therefore, if the information that was left on the hard disk had first been encrypted before it had been viewed by an unauthorized person, it would not be understandable. The actual information, the understandable content, would be safe and secure.

3] One of the most often used services of the Internet is email. It is extremely common for various types of confidential documents to be attached to emails and sent across the Internet. The attached documents could be word processor documents, spread sheets, drawings, etc. These emails are subject to interception by unauthorized people. If the attachment to an email has first been encrypted, then the content has been scrambled. When it is intercepted, the real content of the confidential document is not compromised. In other words, the content is not understandable to the interceptor.

.What Is File Encryption?

Let’s first discuss what a file is. A paper file in your filing cabinet is simply a “collection of information”. It is words, drawings or images on paper. There may be just one sheet of paper in a particular file or there may be many. You can think of a computer file as an electronic version of a traditional paper file. A computer file is stored on some sort of media. This media can be a hard disk, floppy disk, CD, etc.

There are many different types of files on your computer. Files are usually placed in 2 distinct categories: data files and executable files. Some examples of data files are: 1] word processor files, such as letters you wrote to an associate; 2] spread sheets, such as expense reports; and 3] image files, such as logos and pictures.

An executable file is basically a series of instructions to the Central Processor Unit (CPU) of the computer. Some examples of executables files are: 1] a word processor program, or 2] a spreadsheet program.

.How Does File Encryption Work?

Regardless of whether we are referring to a data file or an executable file, file encryption means that you are scrambling (encrypting) the files so that they are not understandable or useable until they have been properly decrypted. File encryption programs such as KetuFile create a scrambled version of a data or executable file.

Why do this? As an example: if you want to send a confidential spread sheet across the Internet and you are concerned that it might be intercepted and read, you should first encrypt it with a program such as KetuFile. In other words, run the KetuFile program, create an encrypted version of the spreadsheet, then send the *encrypted version* as an attachment to an email.

You might have other concerns about the security of your spreadsheet. Perhaps the spreadsheet arrives at its intended location without being intercepted on the Internet, but an unauthorized person gets access to the computer where the spreadsheet has arrived and is able to read it. If, however, the spreadsheet has been encrypted, the unauthorized person will not be able to read it.

.What Is A Key and What Part Does It Play In Encrypting and Decrypting?

In a program such as KetuFile, the Key is a series of numbers and letters that are used to encrypt a file. An example of a Key is:

fH1mvU9IdS3b5Kls

In order for the encryption to take place, this Key is either typed or loaded by another means into a program such as KetuFile. When the party receiving an encrypted file wishes to decrypt to get back the original understandable version, this same Key will be used. The sender (originator) might convey the Key by telephone, fax, courier, etc.

.Conclusions

There are many reasons for security. Often when security is required, it involves keeping information confidential. The vast majority of information today is stored in a computer file format. A file encryption program such as KetuFile can be very effectively used to scramble information so that it is not compromised or revealed to unauthorized persons.