Chapter 6 Encryption

Chapter 6 Objective

This chapter will discuss at a high level encryption and its uses.

6.1 Introduction

As was mentioned in the last chapter and earlier in the book, IT connectivity allows organizations to communicate around the world. Unfortunately, the ability of those wishing to "observe" what the organizations are doing seems to be running slightly ahead of the ability to stop them from doing so. An answer to this dilemma is encryption, which in essence "scrambles" the messages being sent over networks, rendering them unreadable.

6.2 The Information Sent Over Networks

Tyson (2006) notes that there is significant information that often travels over networks that we would not like to share with others, such as:

- Credit card information,
- Social Security numbers,
- Private (intimate, business) correspondence,
- Personal details, such as the names of family members and personal preferences, and
- Bank account information.

To protect the information, encryption systems such as those discussed below may be employed.

6.3 Encryption

Encryption stems from cryptography, the art and science of encoding messages to render them unreadable to those without the key to decode them. Most systems are one of two types:

- Symmetric-key, or
- Public-key (ibid)

6.3.1 Symmetric-Key Encryption

For symmetric-key arrangements two computers are each given the necessary keys to encrypt and decrypt information traveling between the two machines. This is basically a "secret code" between the two machines. The disadvantage, obviously, is that this type of encryption does no good if both machines are not available.

6.3.2 Public-Key Encryption

Public-key encryption is a hybrid of private keys and public keys. The intended recipient of an encoded message provides the sender with a public key, which is known to everyone. The sender encodes the message with the public key and then sends it to the receiver. The receiver then uses their private key (known only to them) in combination with the public key to decode the message.

6.3.3 Digital Certification

"In order to perform public-key encryption on a large scale, such as a secure Web server might need, requires (a specific) approach. A digital certificate is...a bit of information that says that the Web server is trusted by an independent source, known as a certificate authority."(ibid) These authorities, such as VeriSign, are trusted authorities for verifying the authenticity of a sender's certificate.

Important: As will be discussed later in the book, "phishing" websites use fake certificate authority logos to trick unsuspecting users into believing the site is secured by encryption when it is in fact not.