An Introduction to Cryptography

Cryptography is "Art of writing or hiding secret". It is a science of protecting the information from theft or unauthorized access. To do so, important or confidential information is hided as or converted to some other form of gibberish data. Now original information can be recovered only by the right person or application.

Cryptography Objectives

Cryptography is needed in various scenarios varying from simple encryption of a small file to the complicated usages of smart cards used for windows authentications.
Fundamentally, it is used in below mentioned scenarios

- **Data at Motion** - Cryptography is required when communicating over any non trusted medium. This medium can be internet, mobile phones, bank automatic teller machines, wireless intercom systems, Bluetooth devices, wireless microphones and portable storage disks.
  These days, organizations invest heavily to secure all the business communications like emails using cryptographic techniques and products. This is to ensure that no one else other than the trusted recipient can read the message.
- **Data at Rest** - Cryptography is must in securely storing all the sensitive and vital data. This is a basic provision mentioned in most of the compliances which an organization must meet.
  A simple example for this is Encrypting File system (EFS) which is a file system introduced in Windows operating system to provide file system level protection.
- **Data integrity** - Cryptography not only protects the information, but also verifies the integrity of data. This is necessary to ensure that the transferred data has not been tampered by a hacker.
  This is done using the data hashing algorithms, discussed later.

Cryptography Glossary

1. **Key** – In the world of cryptography, “Key” refers to a digital data or file which mathematically determines the output of a cryptographic algorithm when applied to an input message.
2. **Encryption** – Encryption is a process of transforming information, using mathematical algorithms, to some sort of “nonsense” data. To encrypt a message or

plain text, one needs to select an Encryption algorithm and a key (or a key – pair, based on encryption algorithm)

3. **Decryption** – Decryption is the reverse process of encryption, in which the encrypted message is processed and transformed back to the original message. Decryption can succeed if and only if, the correct algorithm (the one used during encryption process) and authentic keys are used.
4. **Digital certificates** – Digital certificates are file used for proving the authenticity of the user or sender. Digital certificates have information about the authority, which has issued the certificate and also, to whom the certificate is issued. Now, there are worldwide trusted certifying authorities (CA) like VeriSign, etc. So, any certificate issued by a Trusted CA, can be trusted as authentic and any information (generally cryptographic keys) contained in the certificate can be safely assumed to be from a trusted source.

Types of Cryptography

There are three main types of cryptography:

1. Secret key cryptography
2. Public key cryptography
3. Hash function

Secret key cryptography – In this type of cryptography, the information is encrypted using a “secret” key. For decrypting the information, the user must possess the secret key. This type of encryption scheme is also known as Symmetric key encryption. In case of confidential data being transferred after encrypted with Symmetric key algorithms, both the sender and receiver must share the secret key. This encryption scheme is preferred over Public key cryptography when a large amount of data is to be encrypted, because it takes lesser time to encrypt or decrypt the data. An example of symmetric key cryptography is the whole disk encryption used by EFS of Windows operating system (EFS).

Public key cryptography – This scheme of cryptography involves two keys or Key-pair, one is a Public key and the other one is private key. Public and private keys are mathematically related and it is impossible to calculate the private or public half of the pair given one key (private or public) of the key pair.
The public key is meant to be distributed publicly whereas the corresponding private key must be kept much secured, ideally in a HSM (Hardware Security Module) device.

If some information is encrypted by a public key, it can be decrypted only by the corresponding private key. Thus, in this scheme, it is not necessary for the sending and receiving users to share the common secret. The recipient distributes his public key. Sender encrypts the data using this public key. Now the data can be decrypted only by the receiver because he only has the correct private key.

Hash functions - Hash functions are one-way cryptographic schemes. In this method, a plain text is processed by the hash algorithm and the output is the hashed value of the original text. From this hashed value, it is impossible to recover the original information. Now a days, Hashing function and algorithms are used in the Authentication module of almost every application including the Windows authentication mechanism.

Source: http://www.go4expert.com/articles/introduction-cryptography-t24529/