**Encryption**

To **encrypt**a file or other [information](http://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) stored in a [computer](http://ecomputernotes.com/fundamental/introduction-to-computer/what-is-computer) means to convert it into a secret code so that it can't be used or understood until it is decoded or decrypted. You might want to encrypt a file if it contained a secret formula for a new invention, or some financial plans that your competitors would love to know about in advance. When you encrypt something, the computer will ask you to set up a password. After that, no one will be able to make sense of the information unless they have the same password.

Encryption hides your data from curious eyes. This is a process of encoding data to prevent unauthorized person from viewing or modifying it. The main features of data encryption are:

1. Prevents unwanted access to documents and e-mail messages
2. Strongest levels of encryption are very difficult to break.

**Process and Types of Encryption**

The process of data encryption consists of certain steps. The data passes through a mathematical formula called an algorithm, which converts it into encrypted data called ciphertext. These algorithms create a key and then encapsulate the message with this key.

 There are two types of encryptions: asymmetric and symmetric.

**Asymmetric Encryption**

In public key (asymmetric) encryption, two mathematically-related keys are used: one to encrypt the message and the other to decrypt it. These two keys combine to form a key pair. Asymmetric encryption provides both data encryption and validation of the communicating parties' identities and is considered more secure than symmetric encryption, but is computationally slower.

A public key encryption scheme has six major parts:

1. **Plaintext -** This is the text message to which an algorithm is applied.
2. **Encryption Algorithm -** It performs mathematical operations to conduct substitutions and transformations to the plaintext.
3. **Public and Private Keys -** This is a pair of keys where one is used for encryption and the other for decryption.
4. **Cipher text -** This is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using key.
5. **Decryption Algorithm -** This algorithm generates the ciphertext and the matching key to produce the plaintext.

### ****The Encryption Process****

The asymmetric data encryption process has the following steps:

1. The process of encryption begins by converting the text to a pre-hash code. This code is generated using a mathematical formula.
2. This pre-hash code is encrypted by the software using the sender's private key.
3. The private key would be generated using the algorithm used by the software.
4. The encrypted pre-hash code and the message are encrypted again using the sender's private key.
5. The next step is for the sender of the message to retrieve the public key of the person this information is intended for.
6. The sender encrypts the secret key with the recipient's public key, so only the recipient can decrypt it with his/her private key, thus concluding the encryption process.

### ****The Decryption Process****

The asymmetric data decryption process has the following steps:

1. The recipient uses his/her private key to decrypt the secret key.
2. The recipient uses their private key along with the secret key to decipher the encrypted pre-hash code and the encrypted message.
3. The recipient then retrieves the sender's public key. This public key is used to decrypt the pre-hash code and to verify the sender's identity.
4. The recipient generates a post-hash code from the message. If the pos~-hash code equals the pre-hash code, then this verifies that the message has not been changed enroute.

### ****Symmetric Encryption****

Private Key encryption (Symmetric), also referred to as conventional or single-key encryption is based on secret key that is shared by both communicating parties. It enquires all parties that are communicating to share a common key. The sending party uses the secret key as part of the mathematical operation to encrypt (or encipher) plain text to cipher text. The receiving party uses the same secret key to decrypt (or decipher) the cipher text to plain text.

Examples of symmetric encryption schemes are the RSA RC4 algorithm (which provides the basis for Microsoft Point-to-Point Encryption (MPPE), Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Skipjack encryption technology proposed by the United S12;tesgovernment (and implemented in the Clipper chip).

An encryption scheme has five major parts:

1. **Plaintext** - This is the text message to which an algorithm is applied.
2. **Encryption Algorithm** - Iperforms mathematical operations to conduct substitutions and transformations to the plaintext.
3. **Secret Key -** This is the input for the algorithm as the key dictates the encrypted outcome.
4. **Cipher text**-This is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using the secret key.
5. **Decryption Algorithm -** This is the encryption algorithm in reverse. It uses the ciphertext, and the secret key to derive the plaintext message.

When using this form of encryption, it is essential that the sender and receiver have a way to exchange secret keys in a secure manner. If someone knows the secret key and can figure out the algorithm, communications will be insecure. There is also the need for a strong encryption algorithm. What this means is that if someone were to have a ciphertext and a corresponding plaintext message, they would be unable to determine the encryption algorithm. There are two methods of attacking conventional encryption - brute force and cryptanalysis. Brute force is just as it sounds; using a method (computer) to find all possible combinations and eventually determine the plaintext message. Cryptanalysis is a form of attack that attacks the characteristics of the algorithm to deduce a specific plaintext or the key used. One would then be able to figure out the plaintext for all past and future messages that continue to use this compromised setup.