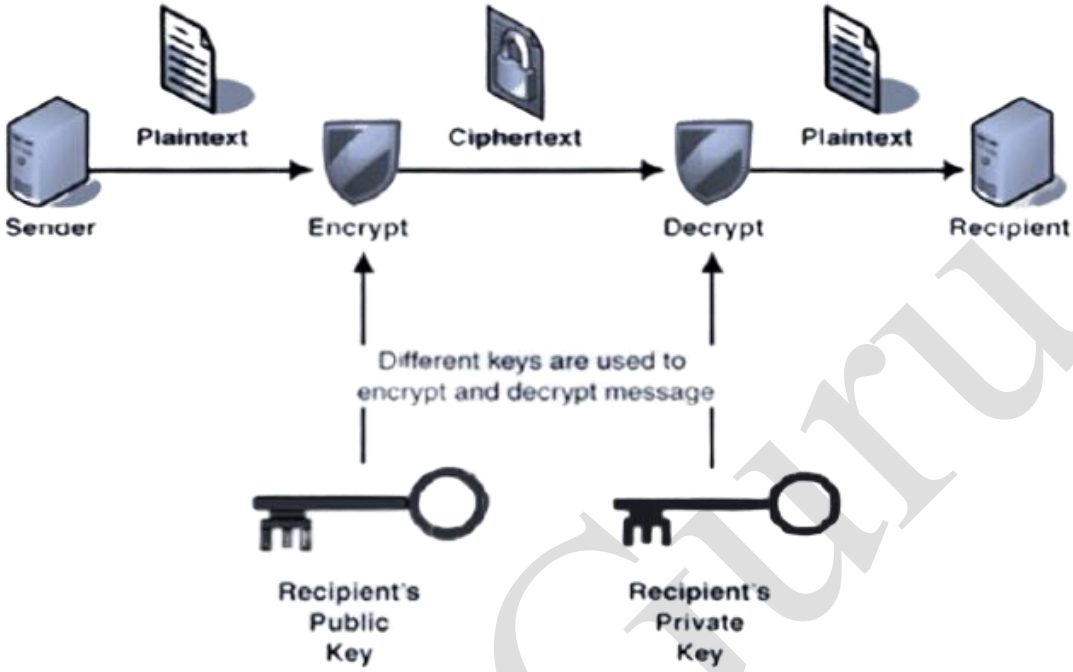
Concept of Encryption and Cryptography



Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting ciphertext back to plaintext.

In other words, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.

It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

Like Cryptography, **Encryption has two modes**: symmetric and asymmetric. A same secret key is shared between the sender and receiver while performing encryption and decryption. The

asymmetric approach, on the other hand, uses two different keys, public and private. Encryption technique is common among the usage of protecting information with civilian system, by governments and military. Customer's personal and banking related data is highly prone to theft, encrypting such files is always a boon, in case of the security system fails to protect the confidential data. Encryption at first may seem like a complicated approach but various data loss prevention software handles it efficiently.

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any opponent. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to use in practice than the best theoretically breakable but computationally secure mechanisms.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for intelligence and agitation has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

Modern cryptography concerns with:

- **Confidentiality** - Information cannot be understood by anyone
- **Integrity** - Information cannot be altered.
- **Non-repudiation** - Sender cannot deny his/her intentions in the transmission of the information at a later stage
- **Authentication** - Sender and receiver can confirm each

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general:

1. Symmetric-key cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

2. Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

3. Public-key cryptography: This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key remains a secret. The public key is used for encryption and for decryption private key is used.

Cryptography vs. Encryption

Basis of Comparison	Cryptography	Encryption
1. Definition	Study of techniques like encryption and decryption.	A process of encoding a message.
2. Nature	Cryptography is a field of study.	Encryption is more of a mathematical operation.
3. Basis	Based on mathematics and algorithms concepts.	Concepts like a cipher, ciphertext, key are used
4. Utilization	Digital signature and security-related algorithms.	Facilitate secret communication.
5. Category	Symmetric and public key Cryptography.	Symmetric and Public key schemes just like Cryptography.
6. Message verification	Cryptography encompasses Encryption including other techniques.	Encryption being a subset of Cryptography using an algorithm – cipher.