**What is Cryptography?**

* Cryptography is the study of securing communication from the outside observers.
* Cryptography is how we can establish secure communication to increase privacy.
* Encryption algorithms take **plain text** and convert it into **cipher text** (format which is not understandable). The user can decrypt the message using key, therefore ensuring that only intended person can read the message.

**Objectives of Cryptography:**

* **Confidentiality:**

Confidentiality means that only intended person can decrypt and read the message.

* **Non-repudiation:**

Non-repudiation means that the sender of message cannot backtrack in future and deny their reason for sending or creating the message.

* **Integrity:**

Integrity means that information in the message cannot be modified while in storage or transit.

* **Authenticity:**

Authenticity means that sender and receiver of the message can verify their identity and the destination of the message.

These objectives help ensure the secure and authentic transfer of information.

**History of Cryptography:**

Cryptography began with ciphers, the first of which was Caesar cipher. Ciphers were a lot easier to solve or explain than modern cryptographic algorithms, but they both use keys and plaintext. Ciphers were simple and less secure encryption methods but today advanced encryption algorithms are more complex and secure. Today there are also some cryptography methods that are irreversible, maintaining the security of the message forever.

**Types of Cryptography:**

Cryptography can be broken into three types:

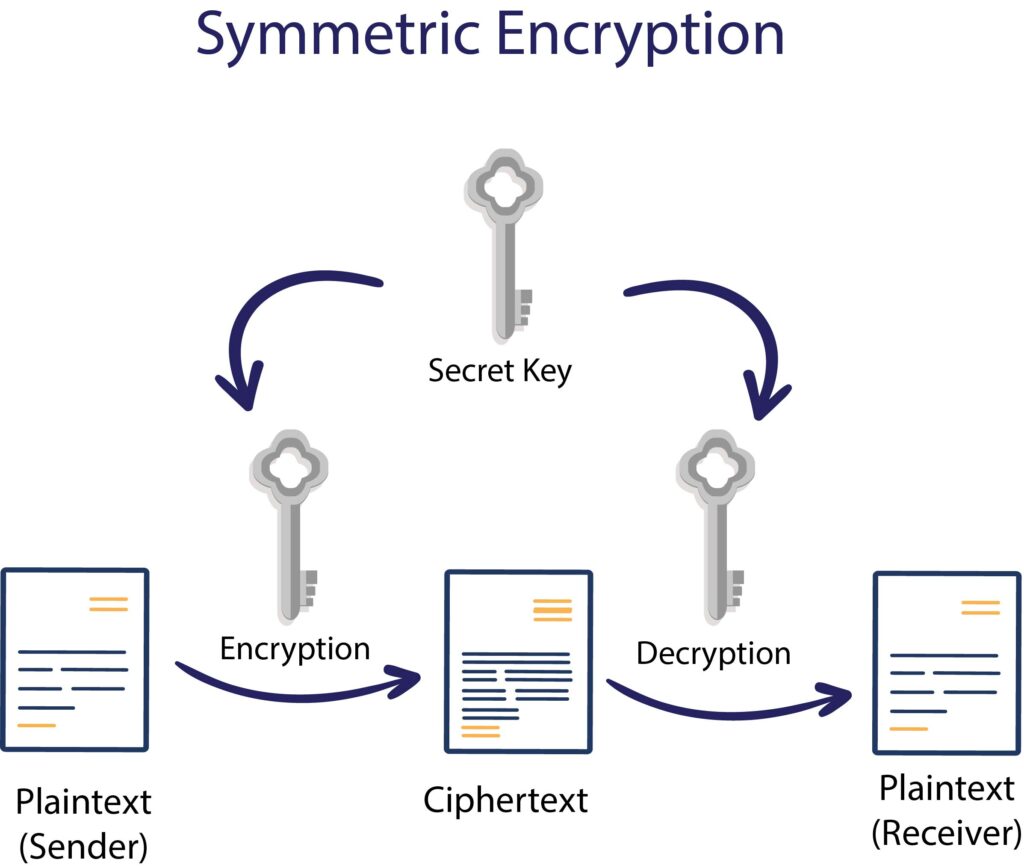
* Secret key cryptography
* Public key cryptography
* Hashing

**Secret Key Cryptography:**

Secret Key Cryptography or Symmetric Cryptography uses same key for both encryption and decryption, making it easiest form of cryptography. It can be used for both **in-transit** and **at-rest** **data** but it is commonly used for **at-rest data**, as the transfer of secret to recipient of message may lead to compromise.

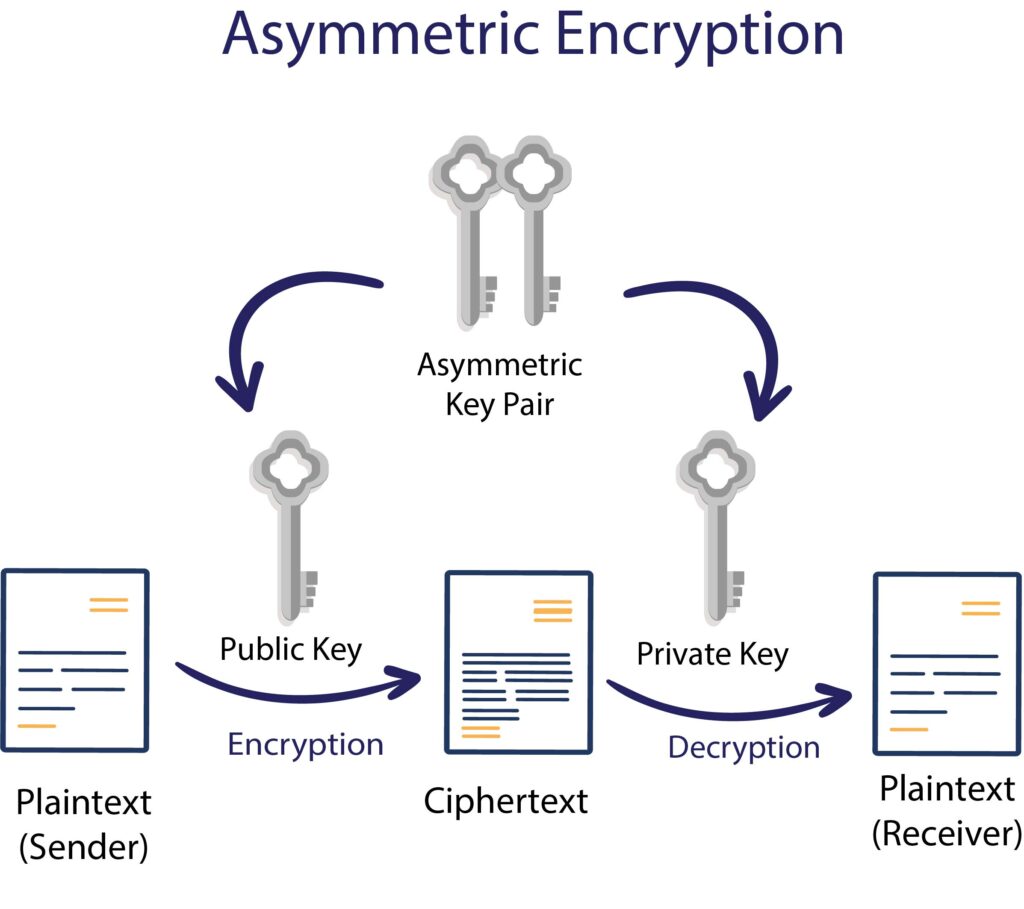
**Example:**

* **AES**
* **DES**
* **CAEASAR CIPHER**



**Public Key Cryptography:**

Public Key Cryptography or asymmetric cryptography uses a pair of keys, one key is used for encryption and other is used for decryption of message. Unlike Symmetric Cryptography, if one key used for encryption of message, that same key cannot decrypt the message, rather the other key shall be used.



One key is kept private and therefore called “Private key” while the other key is shared publicly and can be used by anyone, hence it is known as “Public Key”. The mathematical relation of keys is such that **private key** cannot be derived from the **public key**, but the **public key** can be derived from the private key. The private key should not be distributed and should remain with owner only. The public key can be given to any other entity.

**Example:**

* ECC (Elliptic Curve Cryptography)
* Diffie-Hellman
* DSS (Digital Signature Standard)

**Hashing:**

* Hash function are irreversible, one-way functions which protect the data, at cost of not being able to retrieve the original data.
* Hashing is a way to transform a given string into a fixed length string.
* A good hashing algorithm will produce a unique output for each input given.
* The only way to crack the hash is trying every input, until you get the exact same hash.
* A hash can be used for hashing data (such as passwords) and in certificates.

**Example:**

* MD5
* SHA-1 (SECURE HASHING ALGORITHM)
* SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512.
* SHA-3
* Whirlpool
* Blake 2
* Blake 3