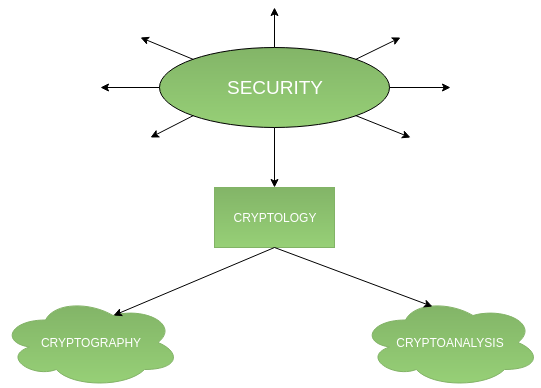
**CRYPTOGRAPGHY**

* **Cryptography** is the study and practice of techniques for **secure communication** in the presence of third parties called attackers.
* **Crypto’ means secret or hidden**.
* Cryptography is the science of secret writing with the intention of keeping the data secret.
* Cryptanalysis - is the science or the art of breaking cryptosystems. Both terms are a subset of what is called **Cryptology.**



**HISTORY OF CRYPTOGRAPGHY**

The history of cryptography begins thousands of years ago.

1. **Classical cryptography** means methods of encryption that use pen and paper and simple mechanical aids. The earliest known use of cryptography is found in non-standard hieroglyphs carved into monuments from Egypt old kingdom.



1. **Polybius**

Each letter is represented by its co-ordinates in the grid. Example “BAT “becomes “12 11 44”



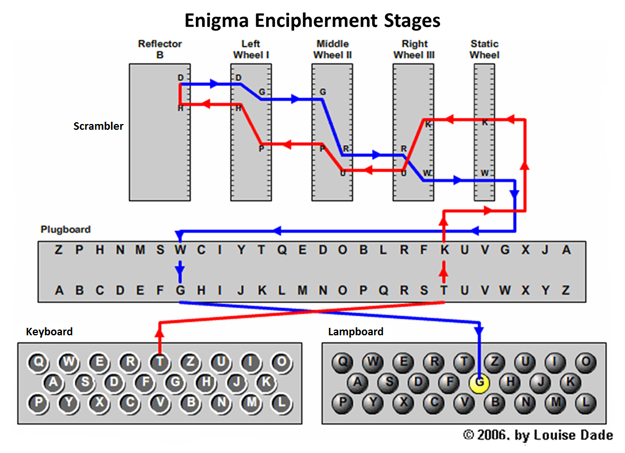
1. **Caesar Cipher**

This method is named after Julius Caesar who used it to communicate with his generals. Also called shift cipher. To encode a message, letters are replaced with a letter that is fixed number of letters beyond the current letter.



1. **Enigma machine**

An **Enigma machine** is a famous encryption machine used by the Germans during WWII to transmit coded messages.  The Enigma machine implemented a **\*substitution cipher**\*, which encrypts a message by substituting one character for another.



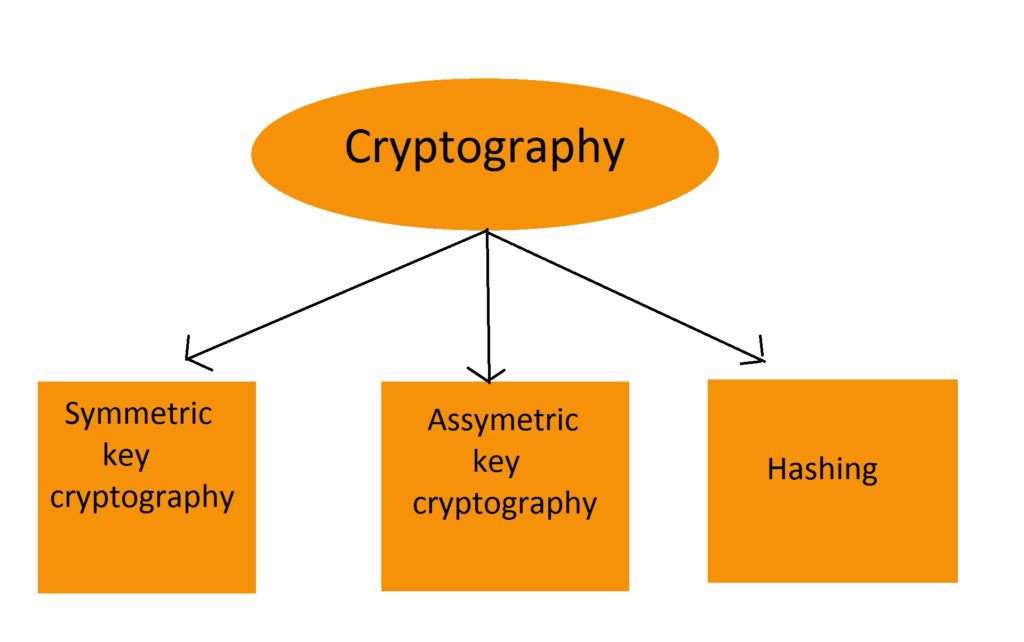
**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called attackers.

1. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.
2. Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by a third party.
3. ***Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.***

**BASIC TERMS OF CRYPTOGRAPGHY**

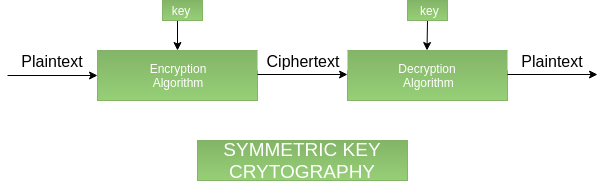
* **PLAINTEXT(P)**
* The original message is known as plaintext.
* Plaintext is in the readable form.
* Plaintext is what you have before encryption.
* **CIPHERTEXT (C)**
* The coded message or encrypted message after encryption is known as ciphertext.
* Ciphertext is in unreadable form.
* **ENCRYPTION (E):** The process of converting plaintext (P) to ciphertext (C) is known as encryption. The algorithm used for encryption is known as encryption algorithm.
* **DECRYPTION (D)**: The process of converting plaintext (P) to ciphertext (C) is known as encryption. The algorithm used for encryption is known as encryption algorithm.
* **SECRET (K)**: A piece of message that is used to encrypt and decrypt the message.

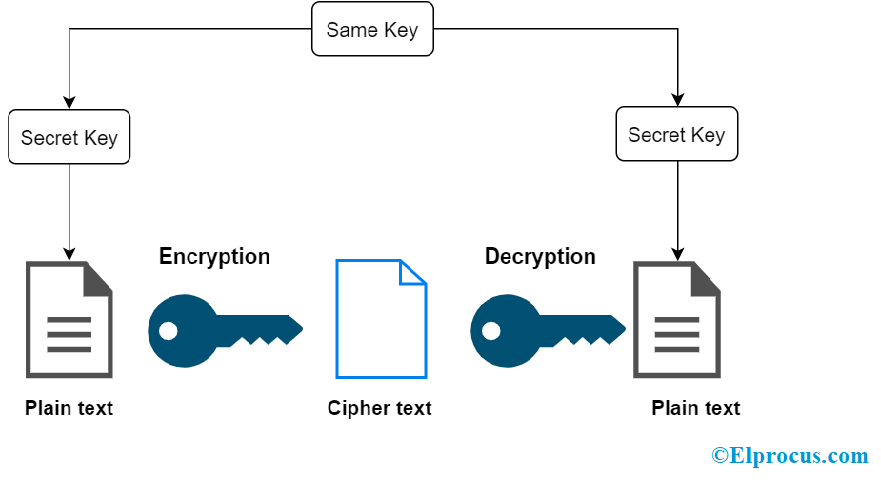
**Cryptography is classified into symmetric cryptography and asymmetric cryptography.**



1. **Symmetric key cryptography –**

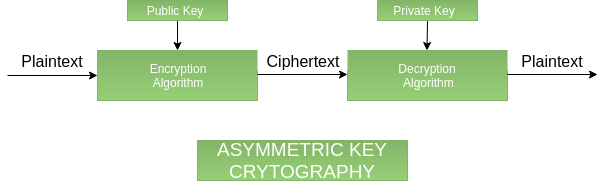
* It involves the usage of **one secret key** along with encryption and decryption algorithms which help in securing the contents of the message. The strength of symmetric key cryptography depends upon **the number of key bits**.
* It is faster than asymmetric key cryptography.
* There arises a key distribution problem as the key has to be transferred from the sender to the receiver through a secure channel.

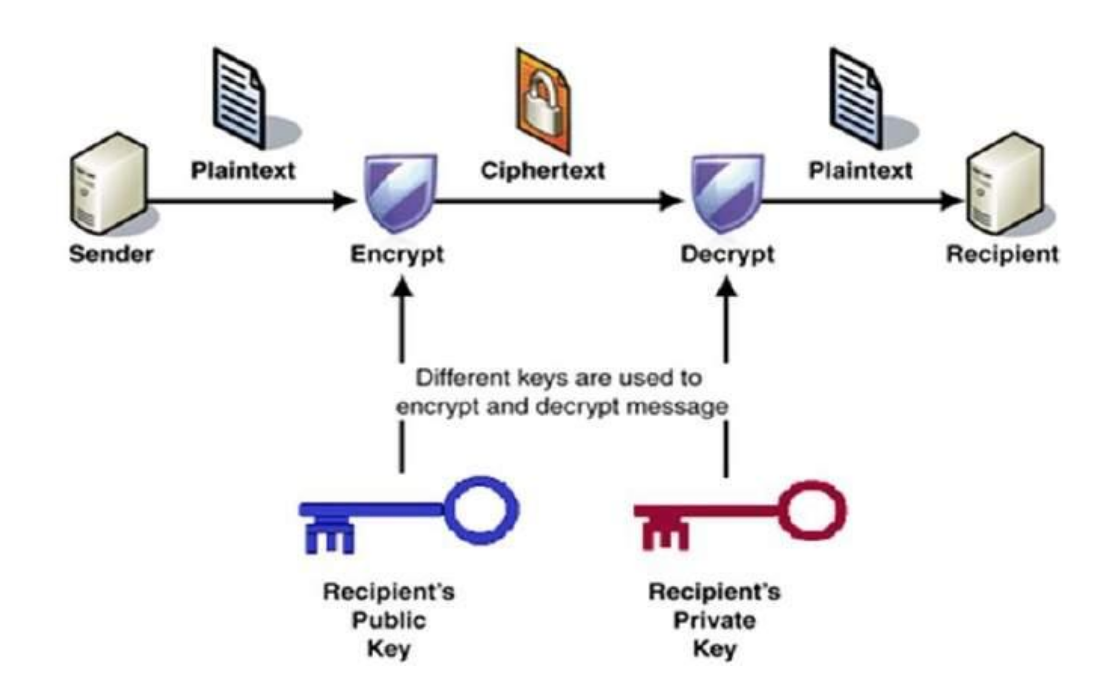




1. **Asymmetric key cryptography:**

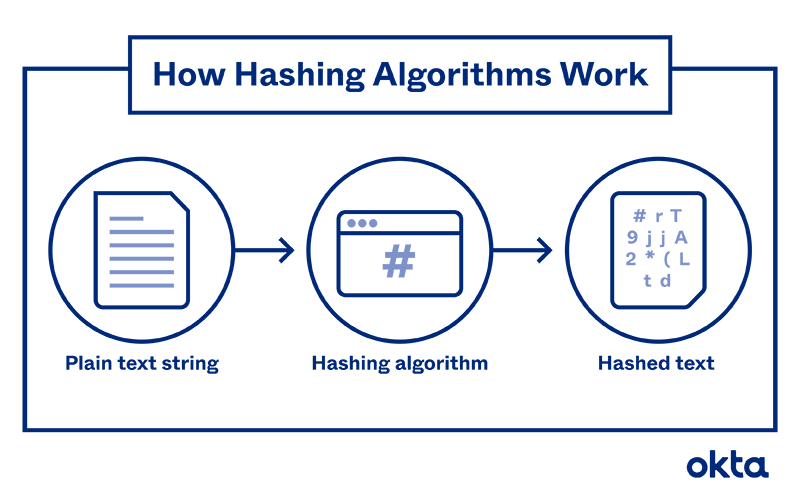
* It is also known as public-key cryptography because it involves the usage of a public key along with the secret key.
* it uses two key along with encryption and decryption algorithms which help in securing the contents of the message.
* it is very slow compared to symmetric key cryptography.

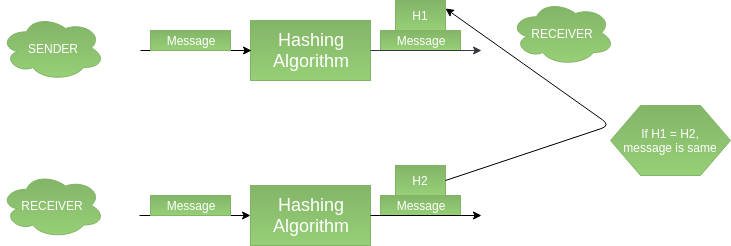




1. **Hashing:**

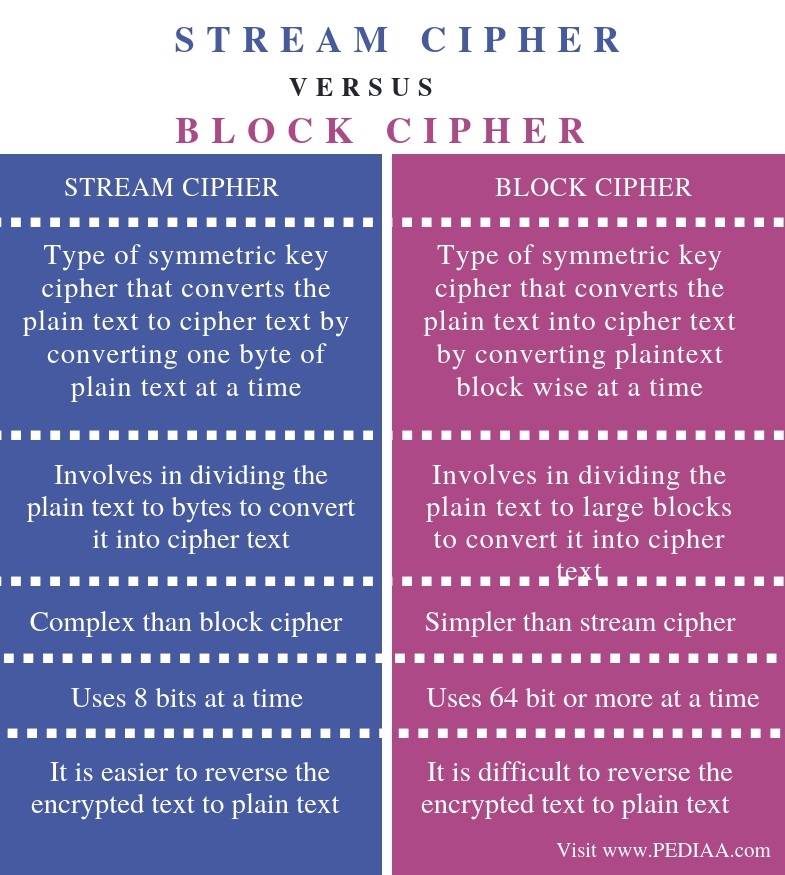
* It involves taking the plain text and converting it to a hash value of fixed size by a hash function.
* This process ensures the integrity of the message as the hash value on both, the sender’s and receiver’s sides should match if the message is unaltered.





|  |  |  |  |
| --- | --- | --- | --- |
| **FEATURE** | **SYMMETRIC** | **ASYMMETRIC** | **HASH FUNCTION** |
| **NUMBER OF KEYS** | 1 | 2 | 0 |
| **LENGTH OF KEYS** | 128 BITS | 2048 BITS | 256 BITS |
| **EXAMPLE** | AES or 3DES | RSA, DSA | SHA-256, SHA3-256, SHA-512  SECURE HASH ALGORITHM |

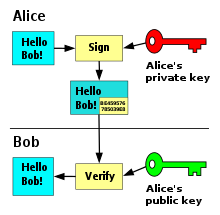
**STREAM CIPHER AND BLOCK CIPHER**





**DIGITAL SIGNATURE**

* A digital signature is **a cryptographic output used to verify the authenticity of data**.
* A digital signature algorithm consists of two operations:
  + **a signing operation**, which uses a signing key to produce a signature over raw data.
  + **a verification operation,** where the signature can be validated by a party who has no knowledge of the signing key.
* The main purposes of a digital signature are:
  + verification of the integrity of the signed data.
  + non-repudiation if the signer claims the signature is not authentic
* Digital signatures rely on asymmetric cryptography, also known as public key cryptography.
* **An asymmetric key consists of a public/private key pair.**
* The private key is used to create a signature, and the corresponding public key is used to verify the signature.



**MAC : MESSAGE AUTHENTICATION CODE**

* MAC stands for Message Authentication Code.
* In MAC, sender and receiver share same key where sender generates a fixed size output called **Cryptographic checksum or Message Authentication code** and appends it to the original message.
* On receiver’s side, receiver also generates the code and compares it with what he/she received thus ensuring the originality of the message. These are components:
* Message
* Key
* MAC algorithm
* MAC value

