Symmetric Vs. Asymmetric Vs. Hash

Symmetric

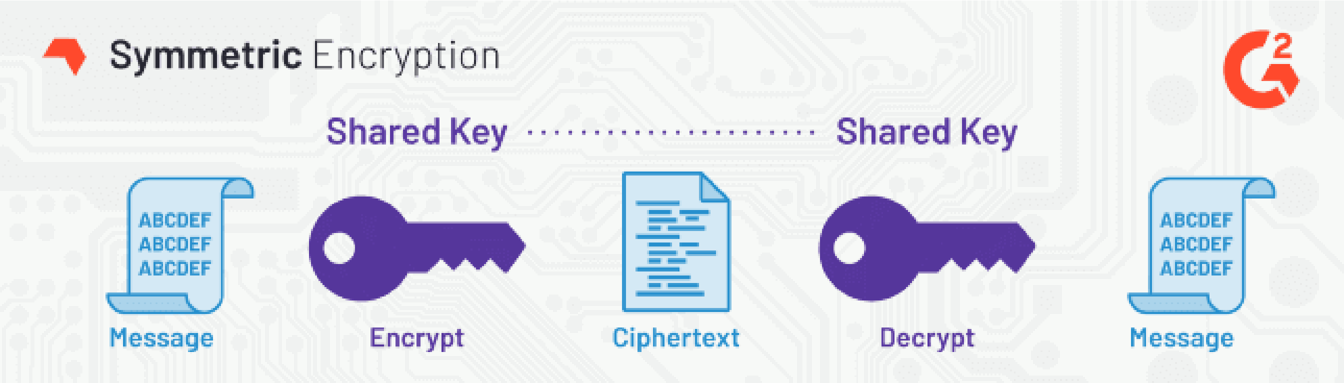
1. In the symmetric encryption method, the sender and receiver use a common key for encryption and decryption, which is not the case in asymmetric encryption.
2. All classical cryptographies are of the symmetric type.
3. Until the 1970s, it was the only type of cryptography.

example : AES,DES

Requirements for secure use of symmetric cryptography

1. Existence of a strong cryptographic algorithm.
2. Existence of a secret key that only the sender and receiver are aware of.
3. The algorithm is assumed to be known to everyone, so there is a need for a secure channel for key distribution.

General mode of operation



The message is given using a key as input to the encrypted algorithm and the encrypted message is generated, the recipient of the message uses the same primary key to decrypte the message and the original text of the message.

Asymmetric

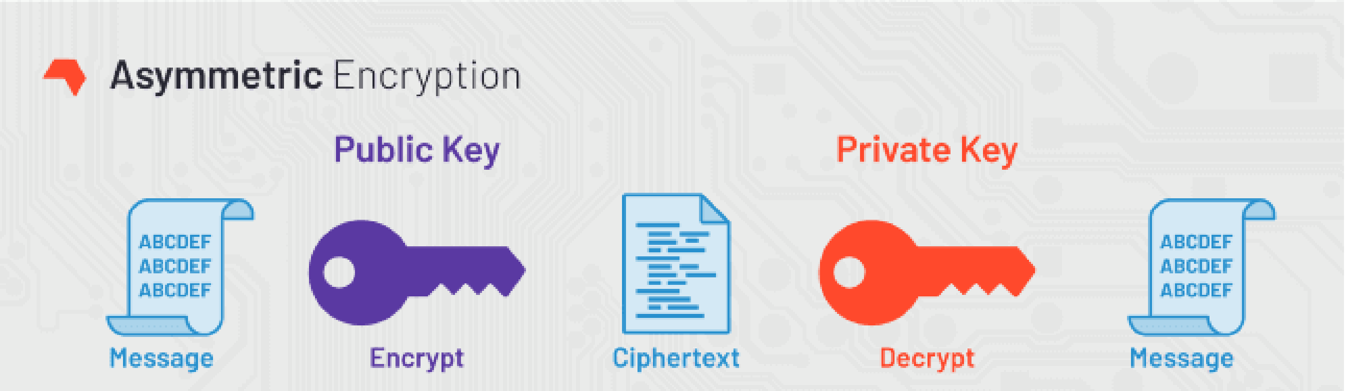
Unlike symmetric cryptography, asymmetric cryptography uses a pair of public keys to encrypt and maintain confidentiality and a private key to decrypt, with a mathematical relationship between them.

example : DSA,RSA,DH,ECC,ECDSA

The use of asymmetric algorithms creates a lot of processing for the CPU during data encryption and decoding. Therefore, instead of using this method to encrypt all information, communication is used in certain stages (such as authentication). One of the reasons this method is called public key encryption is that we make this key publicly available to everyone. Another key used in this method is called private key and this key is not given to anyone and is for the device itself.

It is worth noting that public key algorithms are slower than symmetric encryption algorithms and have longer key lengths.

General mode of operation



Hash

Simply put, a hash means grabbing an input string of any length and giving an output a constant length. Fixed length output is called a hash.

Ideally, when hashing multiple messages, no two different messages should return the same hash. Two different hash messages that result in the same output hash are called ***collisions***.

Hash function features

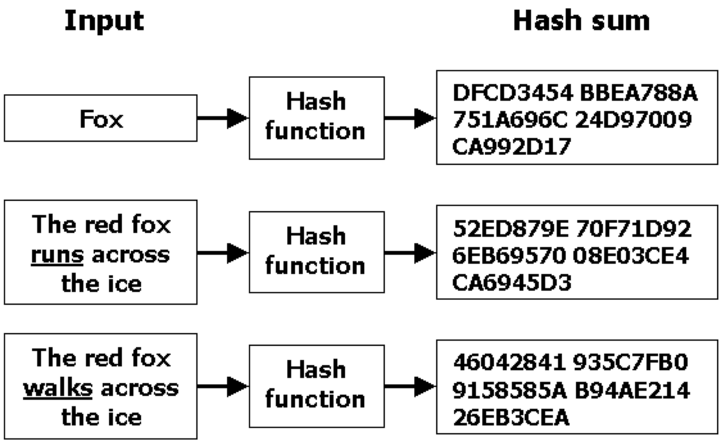
1. **Deterministic**
2. **Quick Computation**
3. **Be one-sided**
4. **Collision resistant**

Types of encryption hash functions

1. *Message Digest (MD MD2 MD4 MD5 , MD6)*
2. *RIPEMD (RIPEND RIPEMD-128 , RIPEMD-160)*
3. *Whirlpool (Whirlpool-0 Whirlpool-T , Whirlpool)*
4. ***SHA (SHA-0 SHA-1 SHA-2 , SHA-3)***

- ***Keccak-256(SHA-3) :***

  Generates 256-bit hashes. Currently used by Ethereum. Keccak is a family of hash functions that is eventually standardized to SHA-3. Atrium called it Keccak instead of SHA-3 because the Hk parameters are slightly different from the current SHA-3. In the world of cryptocurrencies, the SHA-256(BTC) and X11 hash algorithms are the most widely used.


Input
Hash sum
Fox
Hash function
DFCD3454 BBEA788A 751A696C 24D97009 CA992D17
The red fox runs across the ice
Hash function
52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3
The red fox walks across the ice
Hash function
46042841 935C7FB0 9158585A B94AE214 26EB3CEA