Fundamental Concepts of Cryptography for Blockchain

Cryptography: Introduction

- Derived from a Greek word called “krypto’s” which means “Hidden Secrets” and graphein, "to write".
- Art and practice of hiding information.
- Technique of converting a human intelligible data into an unintelligible format.
- It provides Confidentiality, Integrity, and Consistency.

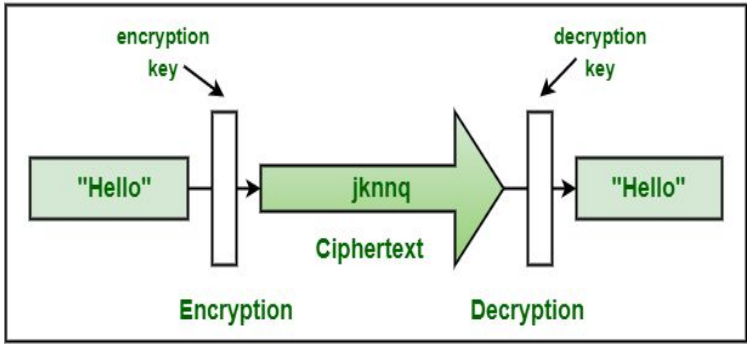


Image source: respective owners

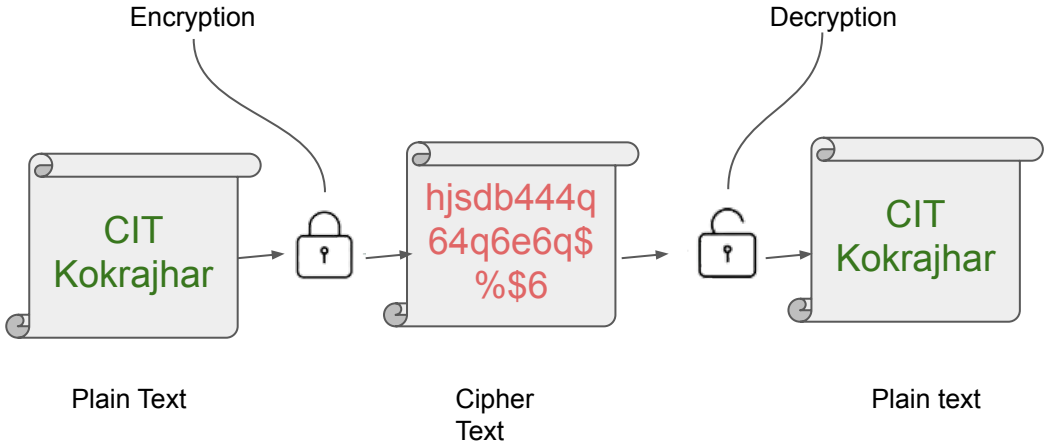
Cryptosystem

A cryptosystem is the five-tuple **P,C,K,E,D** where the following thing are satisfied

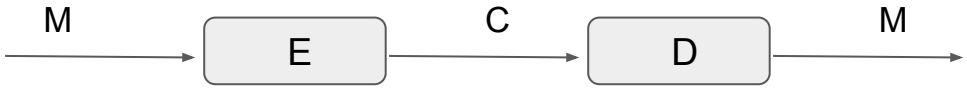
- **P** is a finite set of possible plaintext
- **C** is a finite set of possible ciphertext
- **K** the keyspace, a finite set of possible keys
- **E** is a finite set of encryption functions
- **D** is a finite set of decryption functions

Cryptography: Terminologies

- Plaintext
  - The message.
- Encryption
  - Encoding of message.
- Ciphertext
  - Encrypted message.
- Decryption
  - Decoding of ciphertext



Encryption and Decryption



The following identity must hold true:

$$D(C) = M, \text{ where } C = E(M)$$
$$M = D(E(M))$$

M: Message
E: Encryption
C: Cipher text
D: Decryption

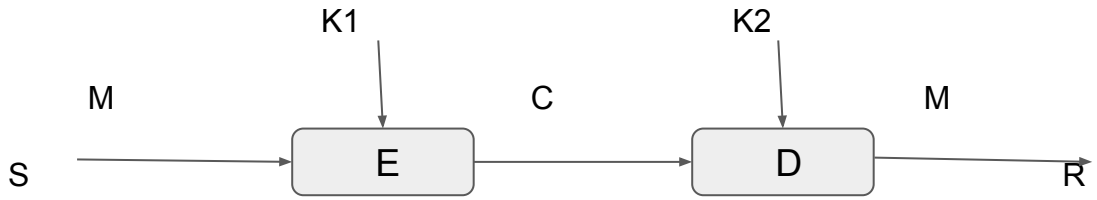
Types of Cryptography

1. Secret Key Cryptography
2. Public Key Cryptography
3. Hash Functions

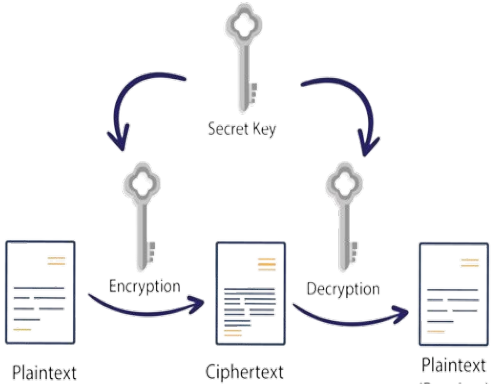
1. Secret Key Cryptography

- uses a single key to encrypt data as well as decryption.
- K1=K2
- Also known as Symmetric key or Private key cryptography.

1. Secret Key Cryptography



K is the secret key shared by both the sender (S) and receiver (R).



1. Secret Key Cryptography

Example

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- Blowfish

Pros.

- Fast
- Block cipher

Cons.

- Key management and Key Exchange
- Weak

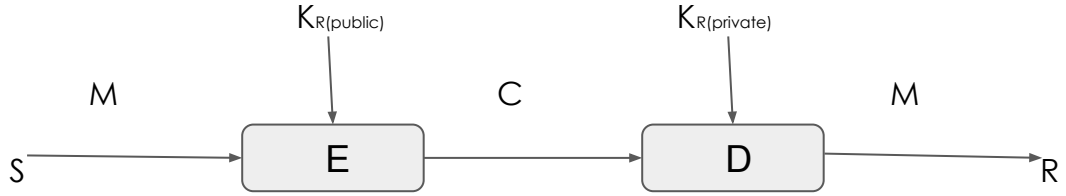
Secrete Key Assurances

- Confidentiality
- Authentication
- Integrity

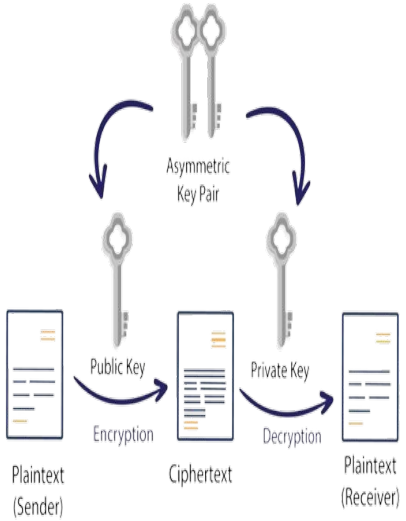
2. Public Key Cryptography

- Uses two keys for Encryption and Decryption.
- Keys are different and not derivable from each other.
- K1 !=K2
- Also known as Asymmetric key cryptography.

2. Public Key Cryptography



$K_{R(public)}$ is Receiver's public key and $K_{R(private)}$ is Receiver's private key.



2. Public Key Cryptography

Example

- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptical curve cryptography)
- DSS (Digital Signature Standard)

Pros.

- Higher Complexity
- Use of key pairs

Cons.

- Slower, computational complex is more

3. Hash Function

- Hash functions are irreversible, one-way functions.
- Hashing is a way to transform a given string into a fixed length string.
- Used for hashing data such as passwords and in certificates.