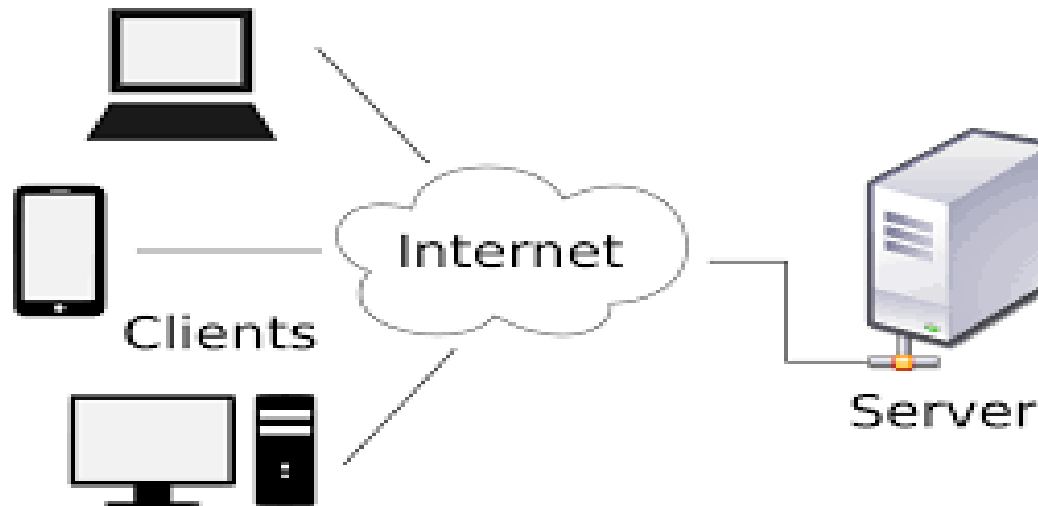


Blockchain Prerequisites

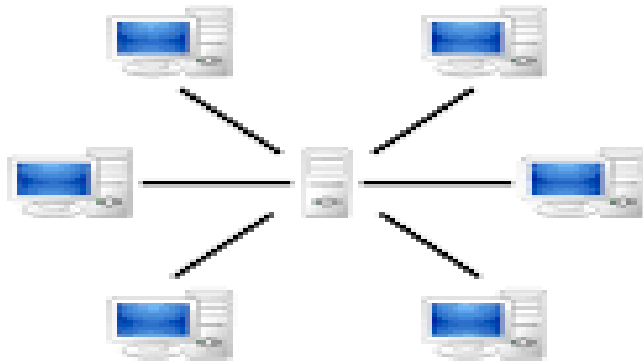
By- Udayveer Singh

Client-Server Model

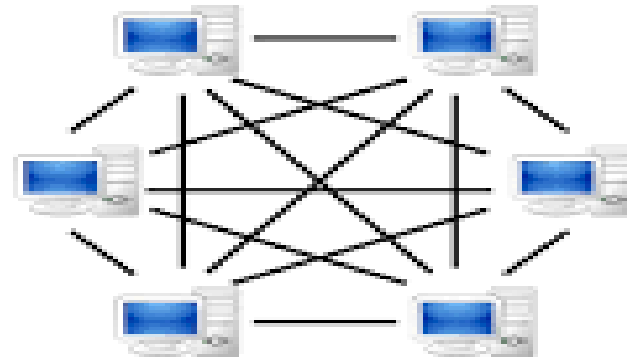


- A normal website is hosted on server.
- Every time a client opens the site, a request is sent to the server and an instance is created for that client.

Peer to Peer Model



Server-based



P2P-network

- In peer to peer network, all the nodes are connected to each other directly.



Cryptography

- Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.
- There are various techniques to convert the readable text to non-readable text.
- Ex- Alejandra -> Bmfkboisb
here i simply used the very next alphabet.
- Encryption and decryption.



Cryptography

- 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



Types of cryptographic techniques

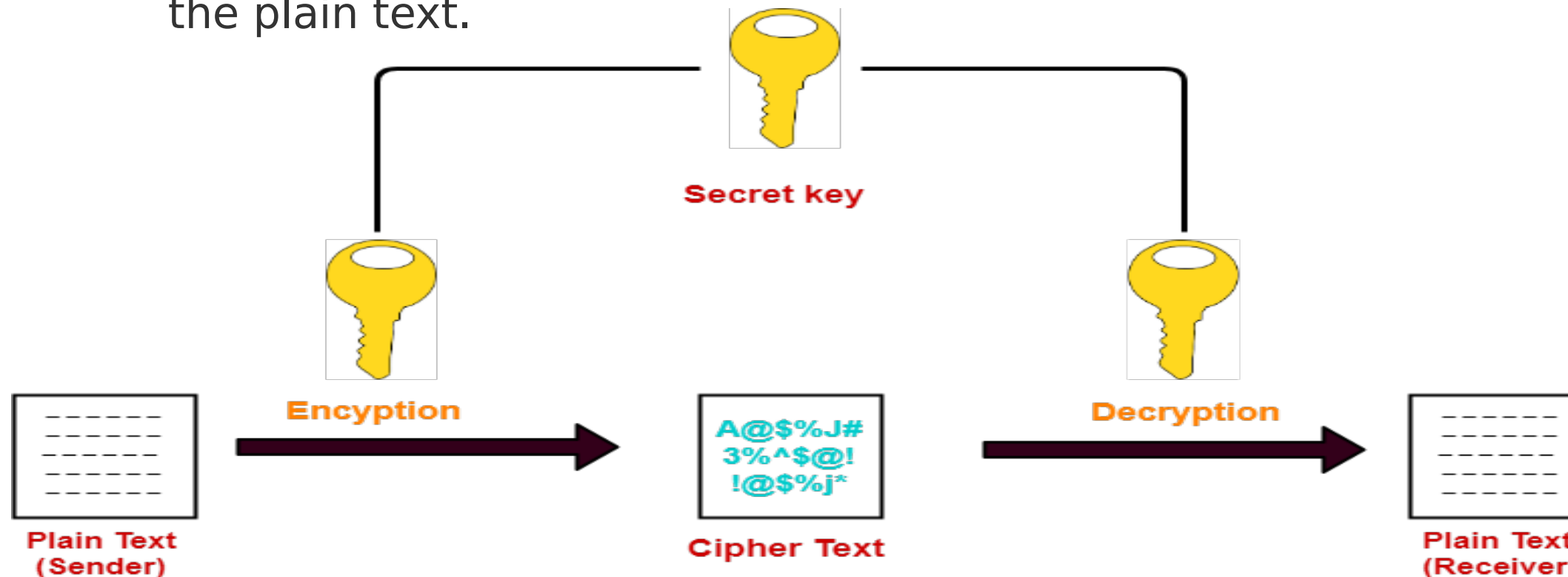
- Symmetric key cryptography
- Hash functions
- Asymmetric key cryptography (Public Key)

Hash Functions

- These are some functions which convert any input into a fixed length output string.
- Example: SHA-256
 - Hello :-
185f8db32271fe25f561a6fc938b2e264306ec304e
da518007d1764826381969
 - HELLO :-
3733cd977ff8eb18b987357e22ced99f46097f31ec
b239e878ae63760e83e4d5
 - Hello :-
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1f
a7425e73043362938b9824

Symmetric Key Cryptography

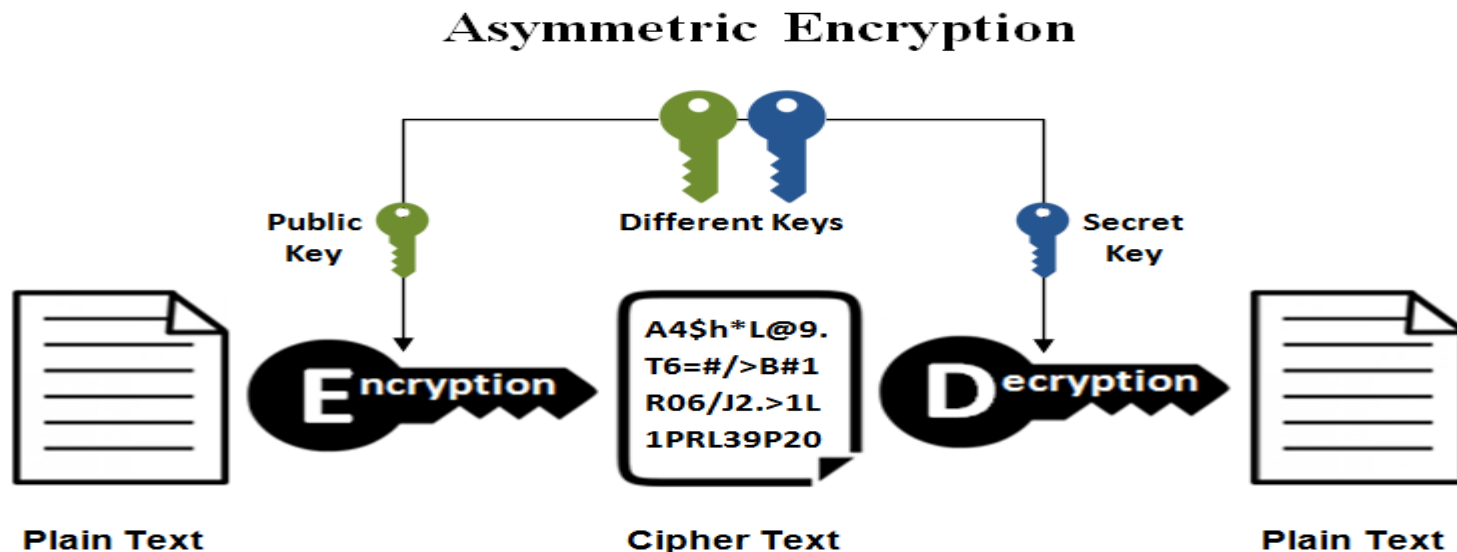
- Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.



Asymmetric Key Cryptography

- 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.

Text1 -> text 2 -> text3



Digital Signature

