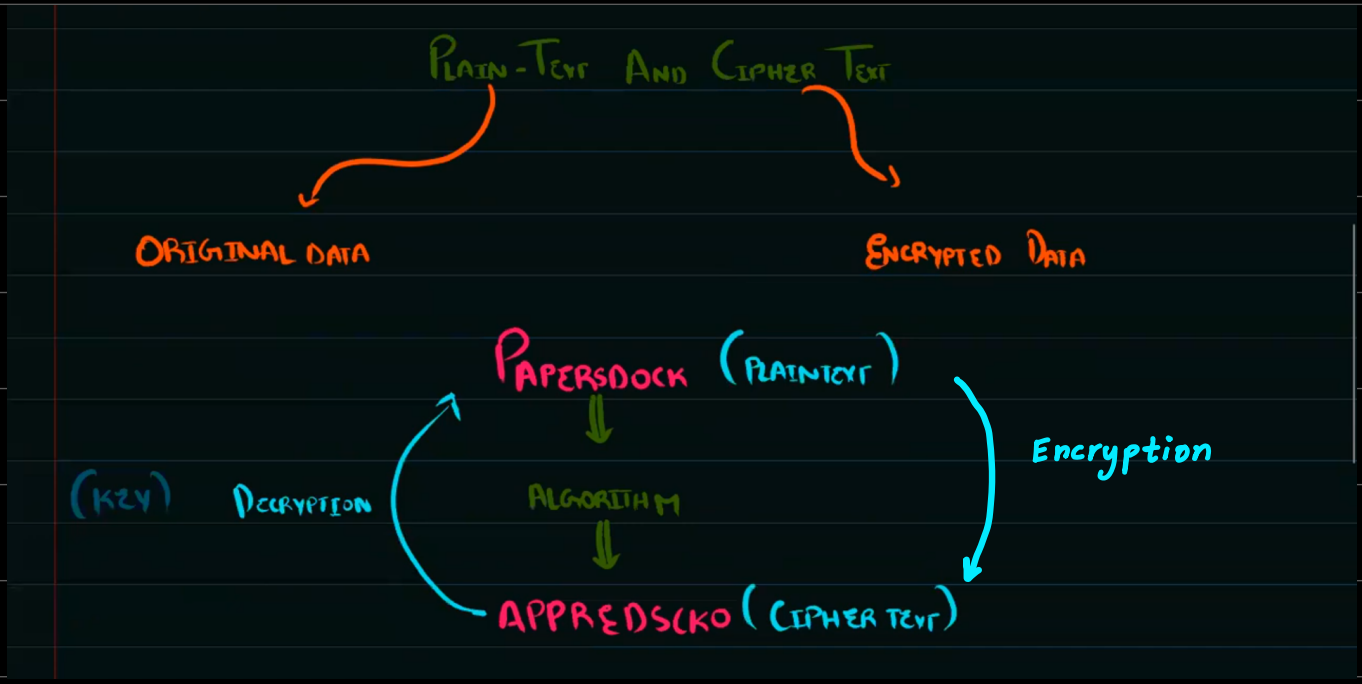
Security

Encryption: It alters data into a form that is unreadable by anybody for whom the data is not intended

- It does not stop the data from being intercepted, but it stops the ↑ (data) from making any sense to the hacker

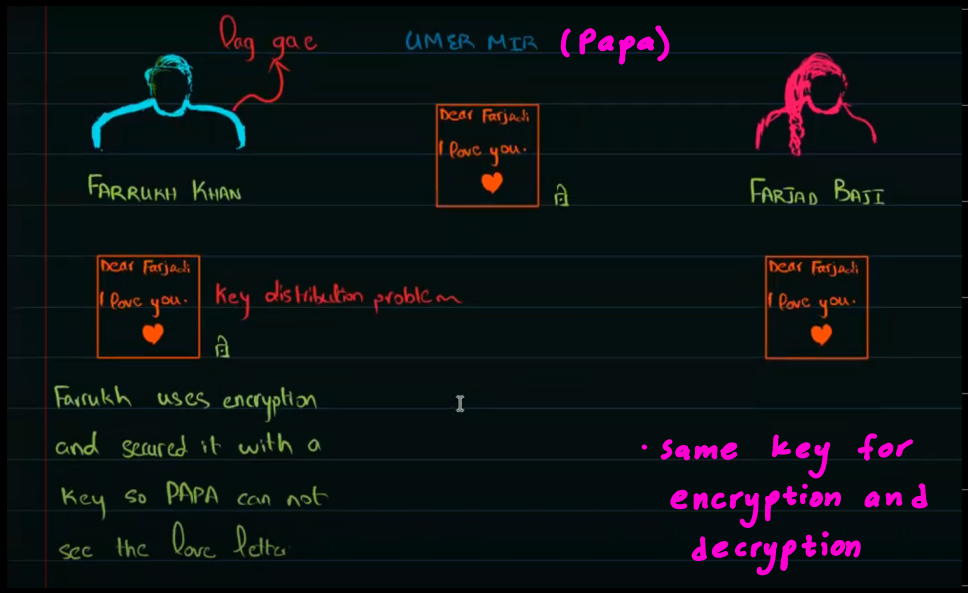


Encryption

① Symmetric Encryption

② Asymmetric Encryption

Symmetric Encryption



Asymmetric Encryption

Plain Text: Original Data

Cipher Text: Encrypted version of the plain text

Encryption: Process of turning plain text into cipher text

Public key: key widely available that can be used to encrypt messages that only owner of the private key can decrypt

Private key: key needed to decrypt the data that has been encrypted by a public key and is used in Assymmetric Encryption and is not shared

Q- What are the similarities and Differences b/w public key and private key?

Similarities:

- Both are used in asymmetric encryption
- As a pair of keys is required
- One is used to encrypt data and the other is used to decrypt the data
- Both use hashing algorithm

Differences:

- Private key only known to the owner of key pair. Public key can be distributed to anyone
- When messages are sent to the owner of public key, they are encrypted with owner's public

key, so they can only be decrypted by owner's private key

- Message digest is encrypted with the private key of the sender to form a digital signature.

Messages are encrypted with the public key of the receiver

Q- Explain how private key and Public key are used to ensure that Ali Wajid is the only person who receives this e-mail.

* Use names in actual question

- Sender's computer will encrypt the email before sending it by receiver's public key
- Receiver will decrypt the email when it is received by using receiver's private key
- As the private key is only known to receiver, so only the receiver can understand.

Q- Explain how asymmetric encryption is used to ensure that the messages remain private

- The sender will encrypt the message with the receiver's public key
- The receiver will decrypt the message with their private key, so the message will remain private

Techniques for secure communication

Q- Explain how the use of asymmetric key cryptography ensures that only a particular person (Person A) can read the email

- Asymmetric Encryption means that the key used to encrypt (public key) is different from the key used to decrypt (Private key)
- Sender will acquire person A's public key
- Sender will encrypt email using person A's public key.
- Sender will send encrypted email to person A
- Person A will decrypt e-mail using his private key.

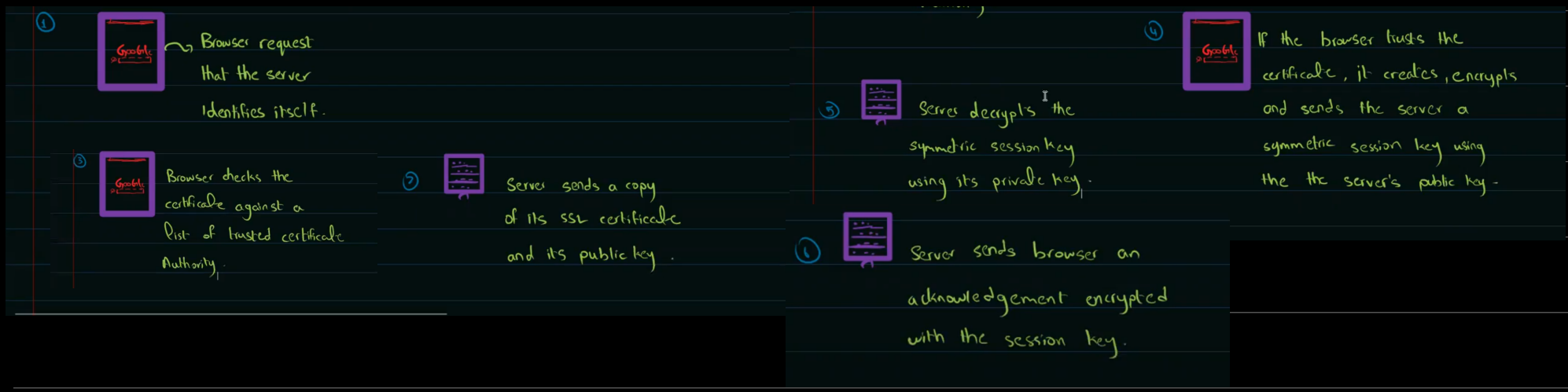
Protocols

① SSL (Secure Socket Layer) ② TLS (Transport Layer Security)

Secure Socket Layer (SSL)

When a user logs onto a website SSL encrypts the data and only the client's computer and the web server are able to make sense of what is being transmitted

Q- Describe what happens when setting up secure connection using SSL (Secure Socket layer)



Q- Explain how the customer's browser and the server which is used to collect the payment will establish a secure connection by SSL?

- Browser requests that the server identifies itself
- Server sends the copy of its Digital certificate
- Containing the public key of the server
- Browser checks the certificate
- against a list of trusted certificate Authority
- If the browser trusts the certificate
- A symmetric session key is created
- This is done by the browser and encrypted using the server's public key and sent to server
- Server decrypts the symmetric session key using its private key
- Server and Browser now encrypt all transmitted data using the session key

Transport Layer Security (TLS)

- Recent Security Protocol
- More secure than SSL
- Only some browsers have the capability to support TLS.
- So that's why SSL is widely used
- It provides encryption, authentication, data integrity in a more efficient way

Layers In TLS

Record Protocol: Can be used with or without encryption, it contains the data being transmitted over the internet (insensitive data)

Handshake Protocol: Permits the web server and client to authenticate each other and to make use of encryption algorithm (used in exchanging sensitive data)

Difference B/W TLS And SSL

- It is possible to extend TLS by adding new authentication methods unlike SSL
- TLS can make use of session caching which improves the overall performance of the communication when compared to SSL.
- TLS seperates the handshaking protocol from the record protocol where data is held

Session Caching

- When opening a TLS session a lot of time is required due to its complex cryptographic process.
- So, the existing session can be used again and again. * Session is stored in memory

Q- What is the purpose of TLS?

- Purpose of TLS is to provide secure communication over a network
- Maintains Data Integrity
- Additional layer of Security
- TLS provides improved layer of Security over SSL
- It is composed of two layers / record protocol and handshake protocol
- TLS protects information by using encryption
- Also allows authentication of servers and clients

1-2 mark

1 point

Application Of TLS:

- Online Banking
- Private E-mail
- Online Shopping
- Online Messaging

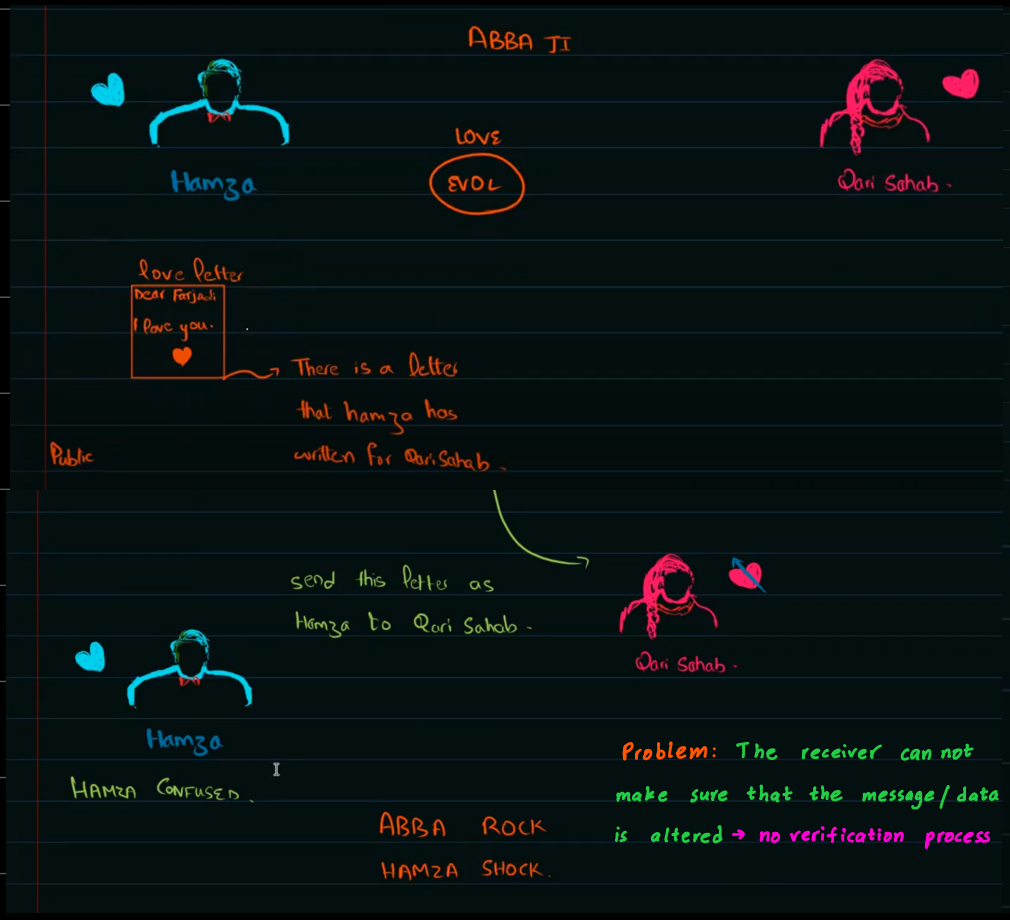
Q- What are the problems that SSL and TLS can overcome?

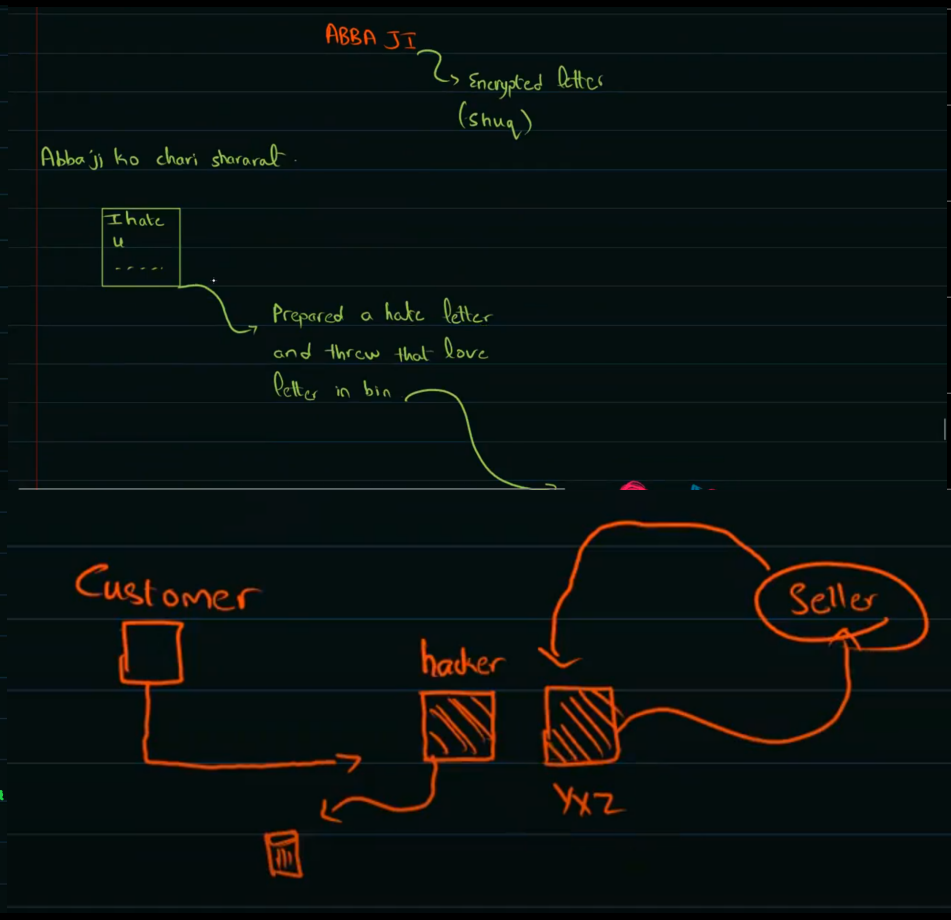
- Security: e.g: alteration of transmitted messages
- Privacy: e.g: Only intended receiver can view the message
- Authentication: e.g: Trust in other party

Q- There are certain security parameters that are agreed on b/w server and client during handshake?

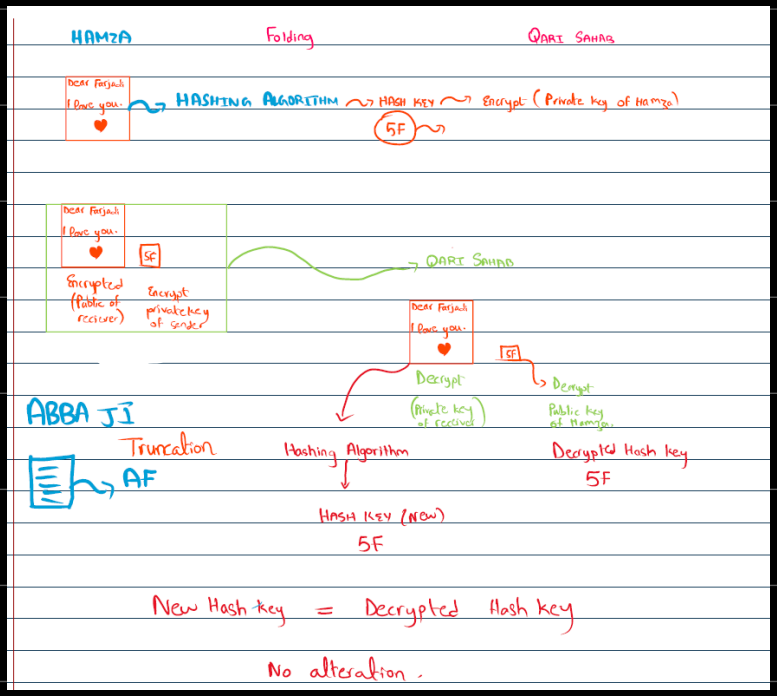
1. Which protocol will be used: As there are different versions of the two protocols
2. Session ID: Uniquely Identifies a related series of messages b/w server and client
3. Session Type: Reusable or not
4. Encryption Method: Asymmetric / Symmetric

Digital Signature And Digital Certificate





Solution



- Sender hashes the letter with the agreed hashing algorithm
- Which provides the hash key
- That hash key is encrypted with sender's private key
- Sender sends encrypted letter with hash key known as message digest
- Receiver already has public key of sender (from digital certificate)
- Receiver decrypts hash key with the public key of sender

- Receiver after decrypting that letter, passes that letter to same hashing algorithm
- If decrypted hash key and new hash key done by receiver is same, then the letter is authentic

Q- What is the difference b/w digital certificate and digital signature

- Certificate is obtained from an issuing authority
- Signature created from a message (Hash key)

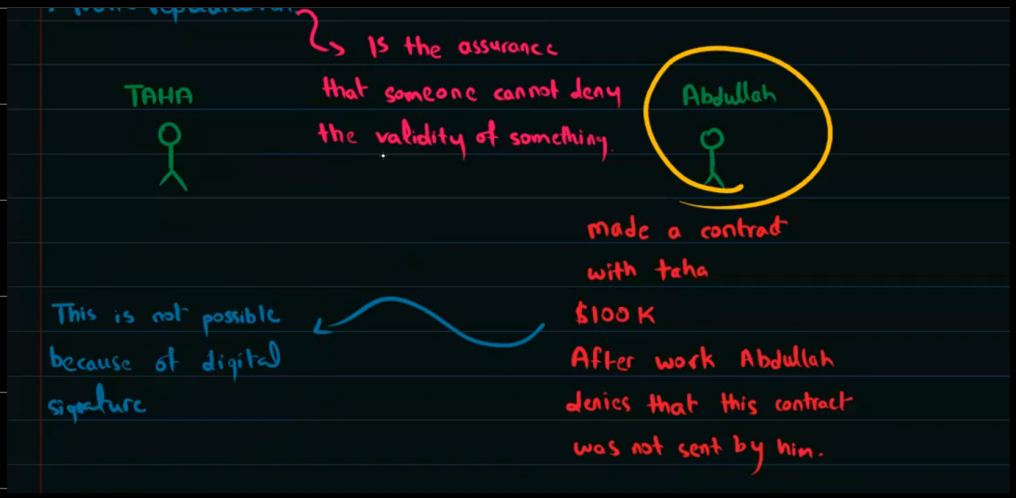
- Certificate provides authentication of owner
- Signature used to authenticate the message that is sent by the owner.

- Certificate remains unchanged while it is valid
- New Signature is created for every message

- Only signature makes use of private key and does not provide information
- Only certificate provides extra information and does not use private key.

Q- What is the purpose of digital signature?

- To ensure a document is authentic / came from a trusted source
- To ensure a document has not been altered during transmission
- Non-repudiation →



Q- How Digital Signature is produced?

- A message is put through agreed hashing algorithm
- To produce a hash total also known as message digest
- Then the message digest is encrypted with sender's private key
- This is how the digital signature is produced

Q- How Digital Certificate is obtained ?

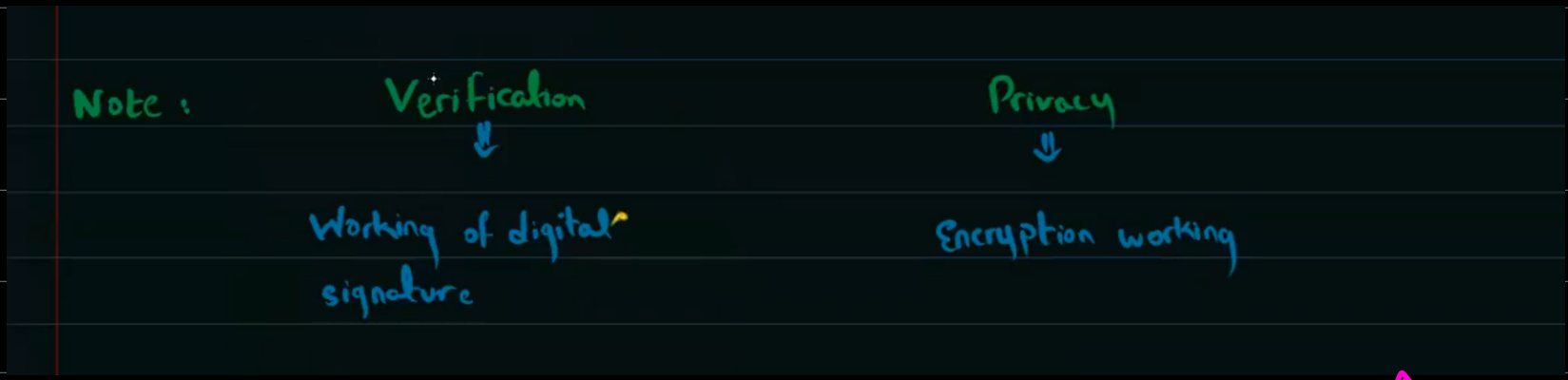
- An application is filled to an issuing certificate Authority (CA)
- with some proof of identity
- for e.g: name of organization / address of organization
- So their identity can be checked by organization registration authority
- So that a digital certificate will only be issued to a trusted organization

Q- What are the items present in a digital Certificate

1. Public key : To encrypt / decrypt data (owner's public key)
2. Agreed Hashing Algorithm: To produce hash total / message digest

- Serial Number
- Name of organization
- Date Valid from/to
- Signature to verify it came from the issuer
- Name of issuer

- Purpose of public key
- Thumb print algorithm
- CA digital signature



Q- Explain how Asymmetric Encryption is used to ensure that it is a verified message

- The sender creates the message digest
- Receiver re-creates the message digest
- If both copies of the message digest match, then the message has not been altered

* Judge answers from marks of question

Q- Explain how asymmetric encryption uses the contents of digital certificate to ensure that the message has not been altered during transmission?

- Sender's message is encrypted with receiver's public key which is provided by the digital certificate of the receiver
- Agreed hashing algorithm mentioned in digital certificate is used on the message to produce the message digest
- The message digest is then encrypted with sender's private key to provide a digital signature
- Both, the encrypted message and the digital signature are sent
- The message is decrypted with receiver's private key
- Sender's digital signature is decrypted with sender's public key (which is provided by the digital certificate of sender)
- To obtain the message digest
- Using the same hashing algorithm, the receiver re-creates the message digest. The two message digests are compared, if they are same then the message is not altered.

Quantum Cryptography
(9618)

Quantum Physics: Is the study of matter and energy at its most fundamental

Photons: Are the smallest possible packets of electromagnetic energy and they carry visible light.

Quantum Computing: Due to advancement in technology, the concept of Quantum Computers has been introduced which will easily be able to crack all the encryption keys

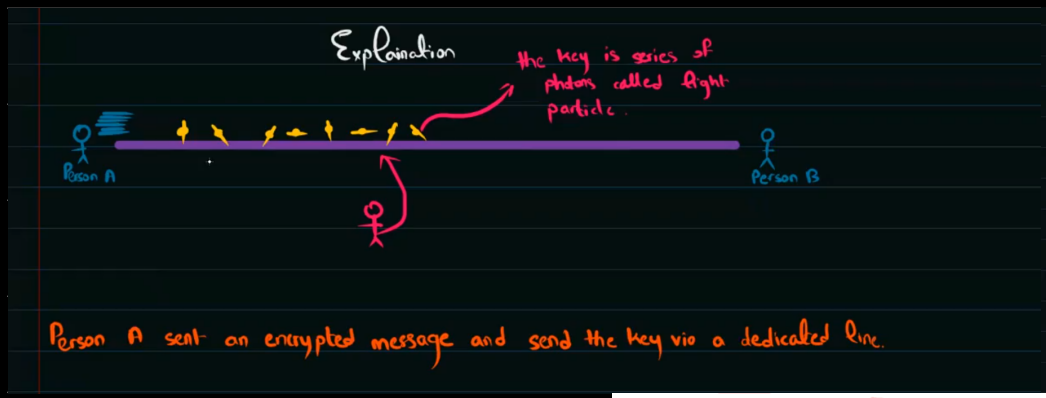
Fight Quantum with Quantum

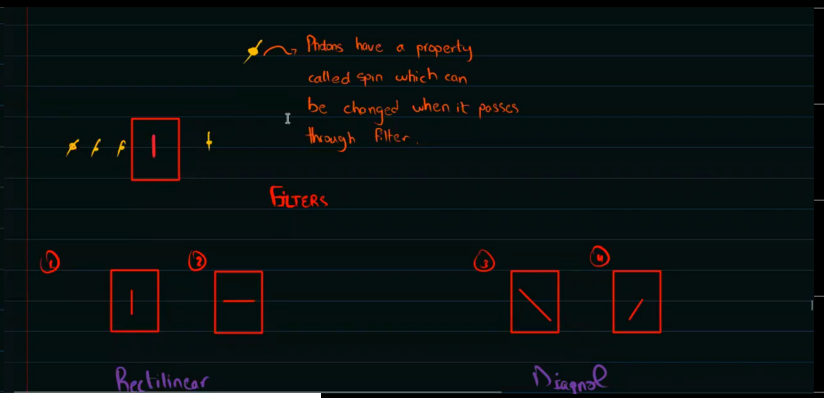
Problem:

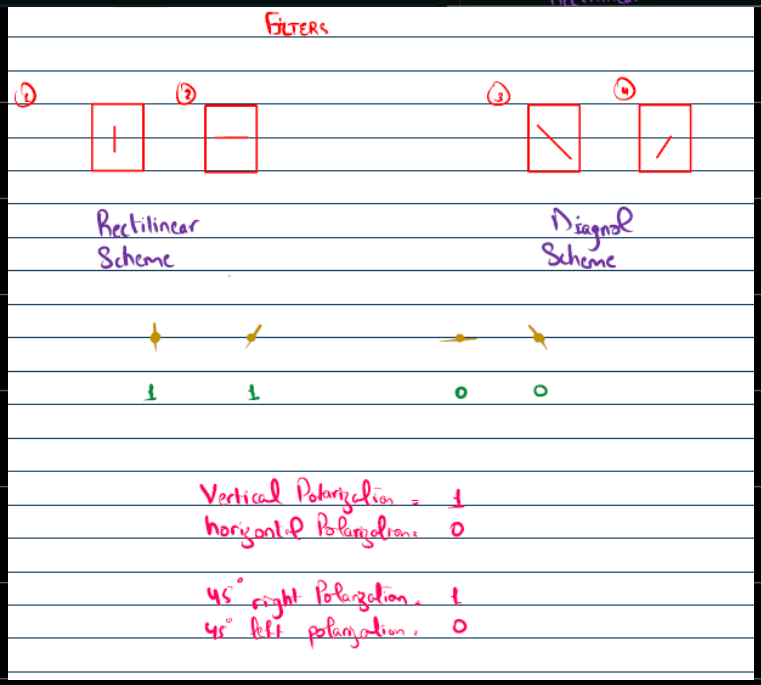
1. Random numbers generation of the code can easily be broken by Quantum Computers
2. Current key distribution techniques will not stand upto a quantum computer

Solution:

- QKD (Quantum key Distribution)

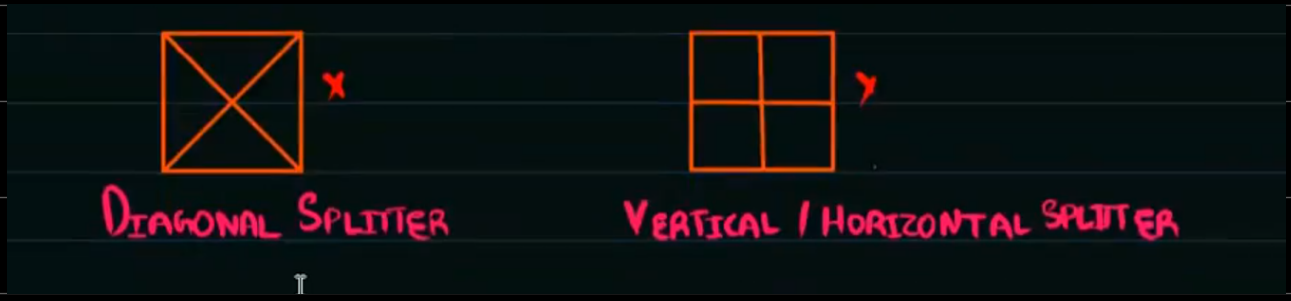






Stages

- The sender uses a light source to generate photons
- The photons are sent through four random polarizers which randomly give one of the four possible polarization and bit values
- The polarized photons travel along a fiber optic cable to its destination
- At the destination, there are two beam splitters (filters) and two photons detectors



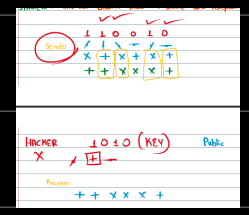
- One of the two beam splitters is chosen at random and the photon detectors are read
- The whole process is repeated until the whole of the encryption key has been transmitted
- The recepient sends back the sequence of beam splitters that were used to sender. e.g:

XXXYYXXYYYYY

- The sender now compares this sequence to the polarization sequence used at the sending

station

- The sender now informs the recepient where in the sequence the correct beam splitter was used
- This now ensures that the sender and recepient are fully synchronized.



Q- What are the benefits of using Quantum Cryptography?

- Any eavsdropping can be identified
- Integrity of the key once transferred can be guranteed
- keys can be exchanged more securely.

Q- What are the drawbacks of using Quantum Cryptography?

- It requires a dedicated line and specialist hardware which can be expensive to implement
- It still has a limited range
- It is possible for the polarization of light to be altered due to various conditions while travelling down fibre optic cable
- Terrorists & criminals can use the technology to hide their activities from government.