SSL AND TLS.

Sunday, 1 November 2020 7:02 PM

3.5

Data exchange over Internet.

ZAFAR Plaintext

4BGBS Ciphertext

Plain text → Cipher text
Encryption (Public key)

Cipher text → Plain text
Decryption (Private key)

---

key terms:

Plaintext: The original text, document or message before it is put through an encryption algorithm.

Ciphertext: The product when plaintext is put through an encryption algo.

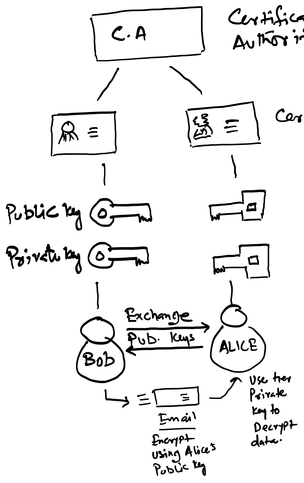
Encryption: It is encoding of plaintext into ciphertext.
There are two types:

Symmetric encryption: It is encryption that uses same secret key to encrypt & decrypt.

Asymmetric encryption: It uses public keys and private keys.

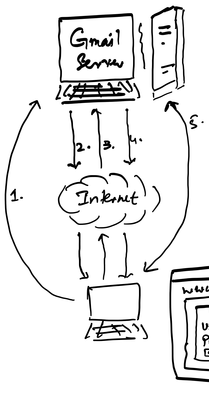
Public key: Encryption/Decryption key known to all users.

Private key: Encryption/Decryption key known to a single user/computer that is owner.



Asymmetric

Secured Socket Layer (SSL)
Transport Layer Security (TLS).



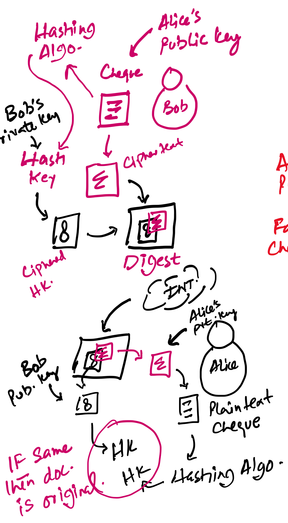
5. Proper Communication starts b/w your computer & server only using session key.

1. Accessed gmail Server as www.gmail.com.
2. Certificate is downloaded over you computer, which contains gmail's public key.
3. Username, password & session key will be encrypted using server's public key & send to Server.
4. Server will use its private key to decrypt msg. and checks un & pas. Further, server will use session key & send a text msg. called welcome msg.

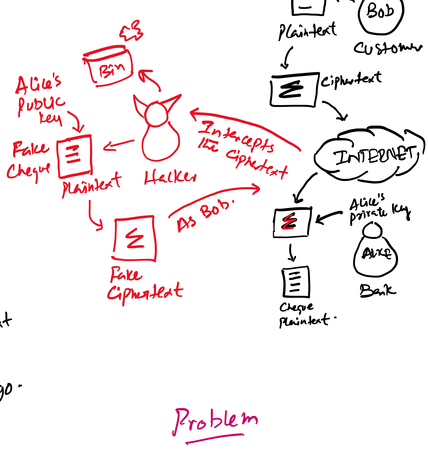
Symmetric

Browser generates a secret key, called session key.

Digital Signatures Authentication (Verification).



Solution



Problem