Subject :

PAGE NO.:
DATE:

Encryption

→ method of transferring readable plain text by converting it to unreadable cipher text. This ensures privacy.
→ Decryption is then used to convert the cipher text to plain text message.

* There are two components of encryption:
  - Algorithm (Public)
  - key (key)

Both collectively decide how plain text will be converted to cipher text.

* Symmetric (AES) algorithm uses only one key. Generally there are options to choose from such as 256-bit AES or 128-bit AES. These are the bit lengths & key-space.
→ The higher the bit length, the stronger the algorithm, and the slower the decryption.
Foreg. 256 AES has 1.1579×10^{77} possible keys
→ This makes it difficult to guess.

Other symmetric encryption algorithms include:
→ Data Encryption Standard (DES)
→ Triple - DES
→ Blowfish
→ RC4 (least recommended)
→ RC5
→ RC6
→ Advanced Encryption Standard (AES) (most recommended)

Subject : _____

PAGE NO.:
DATE:

★ How to get the password to the receiver so that they can decrypt ?

→ Assymetric encryption algorithms use two keys, public & private.

Examples:

1. RSA (Rivest - Shamir - Adleman)
   - most common
2. Elliptic curve cryptosystem (ECC)
3. Diffie - Hellman
4. El Gamal

★ These algorithms solve the problem of agreeing keys. They also allow digital signatures.

Eg. HTTPS uses a public & private key to generate another key for encryption.

∴

→ If message is encrypted with private key, you need the public key to decrypt it and vice-versa.

∴ Benefits & Issues with Assymetric Encryption:

- → Better key distribution
- → Scalability
- → Authentication & Nonrepudiation
- → Slow
- → Mathematically intensive

★ Most softwares use both symmetric & assymetric encryption as a hybrid model.

Hash Functions

Subject :

PAGE NO.:
DATE:

→ To securely exchange keys, we need to authenticate the receiver.
→ A hash function takes the data of any size & it converts it via a cryptographic hash function, to a fixed size string. These output values are called hashes.
→ No authentication or identification of the sender is possible in the one-way hash function.
→ Examples of Hash functions:

- → MD2, MD4, MD5
- → SHA, SHA-1, SHA-256, SHA-512
- → Tiger
- → HAVAL

★ Hashes cannot detect intentional modifications.

Digital Signatures

↳ It is a hash value encrypted with the sender's private key to produce digital signature.
→ a digitally signed item provides:

- authentication
- non-repudiation
- integrity

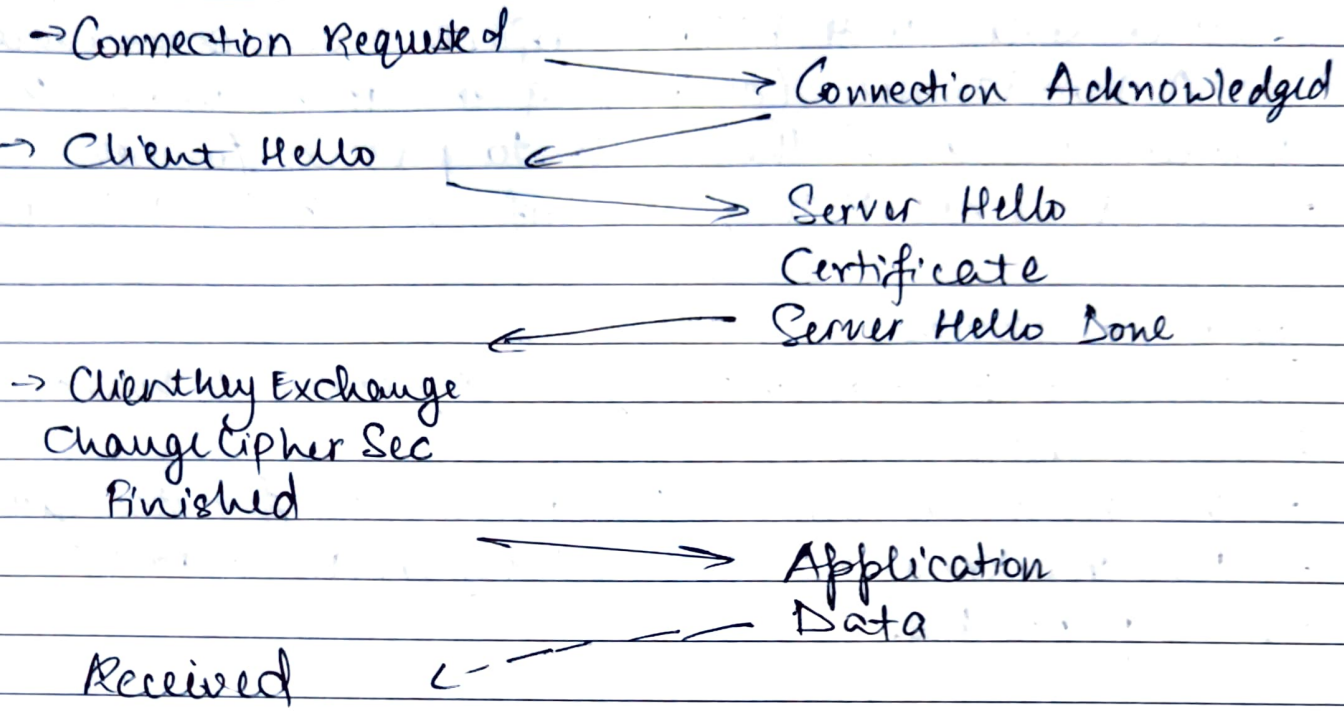
Secure Socket Layers (SSL) & Transport Layer Security (TLS)

↳ These use all the encryption techniques we learnt so far, to make a working security protocol.
→ These are designed to provide communication security over a network.
★ TLS is the most used method for security.

Subject :

PAGE NO.:
DATE:

Eg:



★ The connection is private, authenticated & integrity is maintained.

★ A hacker that needs to hack can stand in between the source & the destination to do SSL Stripping. In which, they can simply change HTTPS connection to HTTP.

→ But SSL stripping is hard. It is difficult to get in the middle.

→ More easier is to hack the client itself.

★ Once SSL is stripped, encryption no longer exists.

Prevention:

- notice HTTPS
- use an encrypted tunnel where SSL strip is not possible.
- dont connect to open networks w/o using VPN.

Subject :

PAGE NO.:
DATE:

HTTPS

↳ HTTP is the application layer protocol.
↳ HTTPS is running HTTP on TLS/SSL. ∴ more secure
↳ Webservers with HTTPS enforce secure communication.
↳ A handshake (exchanging encryption details) happens between a client & the server to proceed further.
→ If it is not HTTPS, the info. will be sent in plain text.

Digital Certificates

↳ Digital certificates use digital signatures & hashes to encrypt for authentication.
→ We need to validate the public key for its legitimacy so that we know no one is sitting in the middle to provide a fake public key.

★ X.509 is a standard that defines the format of public key certificates. These are simply digital documents containing info about owner of certificate. The certificate authority validates that certificate.

★ Vulnerabilities within the ecosystem could enable the creation of bogus certificates.
★ Famous certificate authorities can make mistakes & our browser wont recognize the flaws because of trust.
→ fake certificates can be issued to break HTTPS.

★ Pinning is the process of associating a host with their expected X509 certificate or public key.

★ Steganography: the practice of concealing messages or info. within other non-secret text or data.
- Data is hidden, not encrypted.

Subject :

PAGE NO.:
DATE:

- To perform Steganography:
  - → use any software eg Openpuff
  - → upload file (carrier)
  - → use 3 passwords to hide original file
  - → use 3 passwords to hide a decoy file
  - → if someone forces you to reveal secrets, use decoy password.
  - → otherwise use original password.