Section 17.1 - Encryption, Encryption Protocols and Digital Certificates

Layer 7: Application

Syllabus Content Section 17: Security

S17.1.1 Show understanding of how encryption works

- Including the use of public key, private key, plain text, cipher text, encryption, symmetric key cryptography and asymmetric key cryptography
- How the keys can be used to send a private message from the public to an individual/organisation
- How the keys can be used to send a verified message to the public
- How data is encrypted and decrypted, using symmetric and asymmetric cryptography
- Purpose, benefits and drawbacks of quantum cryptography

`Plaintext`: data before encryption
`Ciphertext`: the result of applying an encryption algorithm to data
`Symmetric key encryption`: one private key is held by both sender and receiver and is used for both encryption and decryption
`Asymmetric key encryption`: there is a public key and a private key one of which is used for encryption and the other for decryption

> encryption

`Symmetric key encryption`: one private key is held by both sender and receiver and is used for both encryption and decryption

- Benifit
  - Simple
  - Quick
- Drawback
  - You have to share your key
  - If someone gets your key then they can read everything

`Asymmetric key encryption`: there is a public key and a private key one of which is used for encryption and the other for decryption

- Benifit
  - Key distribution not necessary
  - Exchange of private keys not necessary
  - Digital signature/message authentication
- Drawback
  - slower because of its longer key lengths

- not to mention that asymmetric encryption calculations tend to be much more complex than their symmetric counterparts.

S17.1.2 Show awareness of the Secure Socket Layer (SSL)/ Transport Layer Security (TLS)

- Purpose of SSL / TLS
- Use of SSL/TLS in client-server communication
- Situations where the use of SSL/TLS would be appropriate

SSL = Secure Socket Layer
TLS = Transport Layer Security
TLS is a version of SSL
SSL is a way to keep your data secure when sending data over the internet.

> `Secure Socket Layer (SSL)`: when its used it becomes an additional layer in the TCP/IP model. It goes between the transport and application layer.

And HTTP will become HTTPS

The stages for SSL are:

1. A client and server make a connection
2. The client and server agree to what encryption to use
3. The client and server may swap digital certificates
4. Once data has been sent, the session is closed.

Steps 1-3 are known as the handshake protocol

SSL uses keys to make sure that

- Your data is private
- You know the person you are sending to (identity authentication)
- Reliability – SSL checks the message

And it uses a mixture of symmetric and asymmetric encryption

S17.1.3 Show understanding of digital certification

- How a digital certificate is acquired
- How a digital certificate is used to produce digital signatures

---

> Digital signatures and digital certificates

1. An individual(A) who is a would-be receiver and has a public-private key pair contacts a local CA.

2. The CA confirms the identity of A.
3. A's public key is given to the CA.
4. The CA creates a public-key certificate(a digital certificate) and writes A's key into this document.
5. The CA uses encryption with the CA's private key to add a digital signature to this document.
6. The digital certificate is given to A.
7. A posts the digital certificate on a website.