17 Security

17.1 Encryption, Encryption Protocols and Digital certificates

Candidates should be able to:	Notes and guidance
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
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
Show understanding of digital certification	How a digital certificate is acquired How a digital certificate is used to produce digital signatures

Unit 17 Security

Syllabus ref. and Key Concepts	Learning objectives	Suggested teaching activities
17.1 Encryption, Encryption Protocols and Digital certificates **(KC3)** **(KC1)**	Define the key terms associated with encryption. Describe the use of encryption, symmetric and asymmetric encryption. Explain the purpose and use of SSL and TLS. Explain how digital certificates are used.	Recap encryption from 6.1 Data security, i.e. purpose and simple encryption algorithms. With learners working in pairs, give one learner the role of sender and the other that of receiver. Get learners to act out symmetric and then asymmetric encryption on a method, sending the message between each other and encrypting and decrypting the message. Discuss the need for secure connections when online and how SSL and now TLS allow for secure transmissions between servers and browsers. Relate back to the use of symmetric encryption and the use of handshakes. Ask learners if they have ever had a website blocked because its digital certificate is invalid, or out of date. Discuss the contents of a digital certificate. Ask learners to find an example certificate online and describe the data items included. **(I)** Give learners facts about the different methods of encryption, the security protocols and digital certificates. Ask learners to identify which method they apply to. **(I)** Put learners into pairs. Give each pair a scenario where data needs to be transmitted securely. Ask them to identify an appropriate method of communication and which method they will use to ensure this is secure. Ask learners to explain their choice to the rest of the class and to justify their decision. **(F) (I)**

Security

Encryption

Symmetric

- Single key
- For encryption and decryption

Drawbacks:

- Key has to be exchanged securely
- If key compromised then messages can be decrypted
- Cannot prove integrity and origin of data

Asymmetric

- Two matching keys
- Public and private
- Share public
- Never share private
- Receiver's public key used to encrypt (produces cipher text)
- Receiver uses private key to decrypt (produces plain text)

Advantages:

- High security
- Allows message authentication
- Detects tampering

TLS/SSL

How it works:

- Protocol with two layers
  - …handshake and record
- Digital certificate used for authentication
- Handshake uses asymmetric cryptography
- Session key is established
- Shared session key used for symmetric cryptography to send and receive data
- Session parameters erased at end

Establishment of SSL(/TLS?) connection between browser and web server:

- Browser requests server to identify itself
- Server sends it digital certificate
- Containing the server's public key
- Browser verifies the certificate against a list of trusted CA's
- If the certificate is valid, a symmetric session key is created
- Browser encrypts the session key with its public key and sends it to server
- Server decrypts the session key with its private key

Appropriate for:

- Accessing secure websites
- Email
- VPN
- VOIP

Digital Certificates/Signatures

Digital Certificate

Electronic document used to prove the ownership of a public key

- Obtained from Certificate Authority
- Contains
  - Owner's public key
  - Hashing algorithm to be used
  - Validity dates
  - Name of CA that issued it
  - CA digital signature

Digital Signature

- Ensures message is authentic
- Ensure message was not tampered with

How it works:

- Message plain text put through agreed hashing algorithm
- Message digest produced
- Digest encrypted with sender's private key to produce the signature
- Receiver will put the decrypted message through the same algorithm and will decrypt the digest with sender's public key
- If the digest produced by receiver is same as decrypted signature, message was not tampered with.

Similarities of certificates and signatures:

- Both used for authentication
- Both use owner's public key
- Both use hashing algorithms

Differences:

- Certificates obtain from CA, signature generated from message
- Certificate authenticates owner, signature authenticates message
- Only signature uses private key

If they ask how digital certificate ensures message has not been altered with during transmission, explain how the message is encrypted, sent, and decrypted and how digital signature is produced and verified. (9608/33/M/J/20)

Quantum Cryptography

Benefits:

- Eavesdropping can be identified due to nature of quantum mechanics
- Longer keys can be exchanged
- Integrity of transferred key guaranteed

Drawbacks

- Difficult to set up
- Limited range