1. Encryption

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

---

Encryption

- Plain text: the original data to be transmitted as a message
- Cipher text: the result of encryption that is transmitted to the recipient
- Digital certificate: An electronic document from a trusted authority that ensures authentication
- Public key: An encryption method produced by a trusted authority that can be used by anyone
  - Key widely available that can be used to encrypt message that only owner of the private key can decrypt
  - Can be used to decrypt a digital signature, thereby confirming the originator of the message
- Private key - Key needed to decrypt data that has been encrypted by a public key

    - Key needed to encrypt data so that it can be decrypted by a public key
    - The key used to asymmetric encryption which is not shared
  - Encryption: Process of turning plain text into cipher text

Main Security concerns:

1. **Confidentiality** is where only the intended recipient should be able to read or decipher the data; the communication must ensure no interception.
2. **Authenticity** is the need to identify who sent the data and verify that the source is legitimate/genuine.
3. **Integrity** is that data should reach its destination without any changes.
4. **Non-repudiation** is that neither the sender nor the recipient should be able to deny that they were part of the data transmission which just took place.
5. **Availability**: Nothing should happen to prevent the receiver from receiving the transmission
   These five words appears constantly in mark schemes; so just write about them if you have no idea about the question

Asymmetric key cryptography

> Encryption that uses public keys and private keys

- Asymmetric encryption uses a matching pair of keys
- A public key (available to everyone)
  - Receiver’s public key used to encrypting the message before it is sent
- A private key (only known to the owner of the key)
  - Receiver’s private key to decrypt the message after it has been received

Benefits:

- Increased message security as one key is private
- Allow message authentication
- Allows non-repudiation
- Detects tampering(篡改)

Symmetric key cryptography

> A single key is used for both encryption and decryption

Drawbacks:

- Key has to be exchanged securely
- Once, compromised, the key can be used to decrypt both sent and received messages
- Cannot ensure non-repudiation

	Public key & Private key
Similarity	- Both used in asymmetric encryption - As a pair of key is required - One is used to encrypt the data and the other is used to decrypt the data - Both hashing algorithms
Difference	- Private key is only known to the owner of the key pair - The public key can be distributed to anyone - When message is sent to the owner of the public key, they are encrypted with the public key - So they could be only decrypted with owner’s private key - Message digest are encrypted with the private key to form a digital signature - Messages are encrypted with the public key of the receiver

Quantum Cryptography/ Quantum key distribution(QKD)

Purpose

- Use quantum mechanics to facilitate the secure transmission of encryption keys

Benefits:

- Any eavesdropping can be identified
- Integrity of the key once transferred can be guaranteed; cannot copied or decrypt at a later date
- Longer/more secure keys can be exchanged

Drawbacks:

- It requires a dedicated line and a specialist hardware, which can be expensive to implement initially
- It still has a limited range
- It is possible for polarisation of light to be altered while travelling down fibre obtic cables
- Due to the inherent security system generated by quantum cryptography, terrorists and other criminals can use the technology to hide their activities from government law enforces

Past paper questions

[

Asymmetric encryption uses different **keys** for encrypting and decrypting data. When Wiktor sends a message to his manager, the message is encrypted into **cipher text** using his manager's **public** key. When the manager receives the message, it is decrypted using her **private** key.

When the manager replies, the message is encrypted using Wiktor's **public** key, and when Wiktor receives the message, it is decrypted into **plain text** using his **private** key.