Explain how tls helps ensure credit details transmitted to the E-commerce server cannot be easily stolen. You should discuss the TLS handshake.

Data is encrptyed

TLS handshake

Browser requests certificate with puvlic key

Browser generates symmetric(session) key

And then encrypts with public key sending to server

Server decrypts with private key

And then uses symmetric (session) key for all subsequent data exchange

g) what is the purpose of a digital certificate

it’s a unique encrypted numerical value of

**Lab Exercise**

William and Ruth are discussing the topic of email security. Ruth recalls the term ‘digital signature’, but cannot remember what it means. She comes to you for help. Briefly explain what it means by a Digital signature and discuss how it can be created and used. **5 marks**