17 Security 计算机安全

17.1 Encryption, Encryption Protocols and Digital certificates 加密，加密协议与数字证书

plain text 明文

data before encryption.

cipher text 密文

the result of applying an encryption algorithm to data.

encryption 加密

process of turning plain text into cipher text by an algorithm using a key.

decryption 解密

process of turning the cipher text back into plain text by an algorithm using a key.

symmetric key cryptography 对称密钥加密

a form of cryptography, in which one (private) key is used for both encryption and decryption.

asymmetric key cryptography 非对称加密

a form of cryptography that provides better security by using a pair of different keys: a public key and a private key. One is used for encryption and the other is used for decryption. Example: RSA.

public key 公钥

the key used in asymmetrical key cryptography that is published by the recipient. The sender **encrypts** the message with the public key before transmission.

private key 私钥

the key used in asymmetrical key cryptography that is never transmitted anywhere. It is used to **decrypt** received message that was encrypted with its matching public key.

quantum cryptology 量子加密

cryptography based on the laws of quantum mechanics (the properties of photons).

Secure Sockets Layer (SSL) 安全套接层协议

security protocol that provides communications security via encryption over the internet. They enable two parties, usually a client and a server, to identify and authenticate each other, and communicate with confidentiality and integrity.

Transport Layer Security (TLS) 传输层安全协议

a more up-to-date version of SSL.

handshake 握手

the process of initiating communication between two devices. This is initiated by one device sending a message to another device requesting the

exchange of data.

digital signature 数字签名

electronic way of validating the authenticity of digital documents (that is, making sure they have not been tampered with during transmission) and also proof that a document was sent by a known user.

digest 摘要

a fixed-size numeric representation of the contents of a message produced from a hashing algorithm. This can be encrypted to form a digital signature.

digital certificate 数字证书

an electronic document used to authenticate the online identity of an individual or organisation behind a website. It is typically issued by a CA, and contains identifying information and a public key.

Certificate Authority (CA) 数字证书授权机构

commercial organisation used to generate a digital certificate requested by website owners or individuals.