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.

asymmetric key cryptography 非对称加密

encryption that provides better security by using a pair of different keys: a public key and a private key. Example: RSA.

public key 公钥

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

private key 私钥

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

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.