Security Tutorial Sample Solutions

Question 1

Generate an RSA key pair from primes 5 and 11.

Sample Solution

- Calculate the product: 55 = 5 x 11
- Calculate the totient: 40 = (5 - 1)(11 - 1)
- Find a co-prime to totient 40: 3
- Choose integers d, i so that d = (1 + 40i) / 3: 27, 2
- The public key is (55, 3)
- The private key is (55, 27)

Question 2

Use the public key generated above to encrypt the message consisting of integer (decimal): 10.

Sample Solution

10^3 mod 55 = 10

Question 3

What does digitally signing a block of data mean? What does digitally signing a certificate allow the checking of? How is a certificate's own reliability checked?

Sample Solution

Digitally signing a block of data means that we take a hash of the data, and then producing a digital signature of the hash using a private key. The signature can be verified by another party who computes the same hash of the data, and verifies the signature using the corresponding public key of the signer.

A digital certificate is a digital document with a corresponding digital signature. The document contains information about the identity of a host, organisation or a person, and their corresponding public key.

Digital certificates are signed by certificate authorities (CAs), who vouch that the identity information is authentic, and that the public-key contained in the certificate belongs to that identity. The certificate can be verified by verifying the signature of the certificate using the CA’s public-key. By verifying the signature of the certificate, we can establish that the identity information in the certificate has not been tampered with, and that it is safe to use the public-key contained in the certificate for confidential communication with the entity described therein. This assumes that we trust the CA to correctly authenticate these details.