INS: Tutorial 7

Question 1

$p = 5$ and $q = 11$

$n = p * q = 55$

$m = (p-1)(q-1) = 4 * 10 = 40$

$e = 3$

$d = 27$

Public key: $(55, 3)$

Private key: $(55, 27)$

Question 2

Public key: $(n, d) = (55, 3)$

$M = 10$

$$\begin{aligned} C &= M^d \ mod \ n \\ &= 10^3 \ mod \ 55 \\ &= 10 \end{aligned}$$

Question 3

In practise, signing a block of data means computing its hash and then encrypting that hash with a private key. The resulting value (the signature) can be used to verify the identity of the sender and the integrity of the data itself. This is done by decrypting the signature with the sender's public key (to reveal the hash they computed), independently computing the hash of the data with the same algorithm, and comparing the two values.

Digitally signing a certificate allows a client to verify that it was issued by a trusted certificate authority (CA) and that its content hasn't been altered since it was signed.

A certificate's reliability is checked by decrypting the signature using the CA's public key to reveal the hash, then comparing this to an independently computed hash. If they match, the identity of the CA and the integrity of the certificate is confirmed. The certificate will also include a revocation URL, which must then be checked to ensure that the certificate (even though it may have passed integrity checks) has not been revoked.