23-S2-Q1

Q (a) RSA work

pri. pub.

SSL / TLS 1.2

(b) RSA signature VS RSA encryption

3, 1 Bob: pub: 7

(i) Bob - pri. ?

(ii) m = 9 Bob

Solution: (a) RSA works

① key generation

Two large primes p and q are generated

compute $n = p \times q$

compute $\phi(n) = (p-1) \times (q-1)$

select at random the encryption key e,

where $1 < e < \phi(n)$

e should be a prime number

e and $(p-1)$ and $(q-1)$ should not have common factors.

② Solve following equation to find decryption key d

$e \cdot d \bmod \phi(n) = 1$ and $0 \leq d \leq n$

publish the public encryption key e

keep secret private decryption key d

③ RSA USE

(1) the sender to encrypt a message m

obtains public key of recipient e

computes $C = M^e \bmod N$, where $0 \le M < N$

(2) the owner to decrypt the ciphertext C use their private key d computes $M = C^d \bmod N$

(a) RSA in SSL/TLS 12

① key exchange:

the shared secret is decided by the client, who then encrypts it with the server's public key (extracted from the certificate) and send it to the server

(b) Differ

Encryption: sender uses recipient's public key to encrypt, recipient decrypts with the private key.

Signature: signer uses their own private key to sign; anyone can verify the signature

using the signer's public key.

(i) RSA compute. Bob secret key

$p = 3$, $q = 11$

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

$e = 7$

$e \cdot d \bmod \phi(n) = 1$

$$d = \frac{k \cdot \phi(n) + 1}{e}$$

$$d = \frac{20k+1}{7}$$

$k = 1$, $d = \frac{21}{7} = 3$

So, the Bob private key is 3.

(ii) Encryption $m = 9$ by Alice

$c = m^e \bmod n$

$= 9^7 \bmod 33$

$= 15$

Decryption by Bob

$m = c^d \bmod n$

$= 15^3 \bmod 33$

$= 9$