

Solutions to Assignment 5

Question 1

Alice's public key: $Pk_A = g^{x_A} \pmod{p} = 5^3 \pmod{47} = 31$.

Bob's public key: $Pk_B = g^{x_B} \pmod{p} = 5^7 \pmod{47} = 11$.

For performing the Diffie-Hellman key agreement, Alice and Bob will do the following computations:

- Alice computes: $k_{AB} = Pk_B^{x_A} = 11^3 \pmod{47} = 15$.
- Bob computes: $k_{AB} = Pk_A^{x_B} = 31^7 \pmod{47} = 15$.

Therefore, Alice and Bob obtained the shared key $k_{AB} = 15$ as a result.

Question 2

Bob can generate a digital signature using the RSA scheme as follows:

- Bob creates his public key and private key pair, for example, $(e, d) = (3, 147)$.
- Bob computes $h(m) = 2m \pmod{n} = 2 \times 2 \pmod{253} = 4$.
- Bob computes $r = h(m)^d \pmod{n} = 4^{147} \pmod{253} = 49$, which is Bob's RSA signature on the message m .

Question 3

(a) Bob can generate a DSS signature of the message m as follows:

- Randomly pick a state generated by PRSG: $k = 10, 0 < k < 32$.
- Compute $r = (g^k \pmod{p}) \pmod{q} = (2^{10} \pmod{47}) \pmod{23} = 37 \pmod{23} = 14$.
- Compute $h(m) = 2m \pmod{p} = 2 \times 101 \pmod{47} = 14$.
- Solve for s in the equation: $h(m) \equiv xr + ks \pmod{q} \Rightarrow s = k^{-1}(h(m) - xr) \pmod{q} = 10^{-1}(14 - 5 \times 14) \pmod{23} = 22$.

Therefore, the pair $(14, 22) = (01110, 10110)$ is a DSS signature of the message $m = 101 = 1100101$.

(b) If the random number k used in the DSS signature is compromised, then an attacker can recover the signer's private key when he intercepted the corresponding message m and signature (r, s) . More specifically, the attacker can find the signer's private key by solving the following linear congruence equation:

$$x \equiv r^{-1}(h(m) - ks) \pmod{q}.$$

(c) Since the signature verification requires the computation of $s^{-1} \pmod{q}$. If $s = 0$, then s^{-1} does not exist. To avoid this situation, the signer needs to check that $s \neq 0$. Another reason is that if $s = 0$, an attacker can obtain the signer's private key x by computing $x \equiv r^{-1}h(m) \pmod{q}$.

(d) If the hash function is not secure in *DSS*, then an attacker can easily find another message m' such that $h(m) = h(m')$. Therefore, the attack can replace the message m by m' and the resulting message and signature tuple $\langle m, (r, s) \rangle$ will also pass the verification of the verifier.

Question 6

(a) After Bob submits his public key to CA, the CA will generate a certificate for Bob which binds between Bob's public key and his identity. Let Pk_{Bob} be Bob's public key, ID_{Bob} be Bob's identity, T_{Bob} be the expiration date of Bob's certificate, S be the scope (enc or sign). Then Bob's certificate has the following format:

$$\text{certificate} = \langle Pk_{Bob}, ID_{Bob}, T_{Bob}, S, \text{RSASign}_{CA}(Pk_{Bob}, ID_{Bob}, T_{Bob}, S) \rangle.$$

(b) Alice should first obtain Bob's certificate and check whether it is valid by verifying the CA's signature. Furthermore, Alice also needs to communicate with the CA to ensure that Bob's certificate has not been revoked before the expiration date.

(c) A certificate authority (CA), which issues digital certificates for use by other parties, is the trust root of a public-key system. Users establish the trust relationship among themselves through verifying certificates issued by a CA.