George Jone

913177426

Due: 7:00PM, Tuesday, 03/15/2016

CSC650 Secured Network Systems

Homework 2

1.

   a. No, hashes can easily be generated. Anybody can change the message and append it with another hash. The receiver can't detect this modification. Bob's solution won't solve the problem.
   b. The right way to construct a message authentication code is with a secret key.

2. p = 23, q = 17, and e = 5, N = pq = 391, d = ?

   $\varphi(n) = (p - 1)(q - 1) = 22 * 16 = 352$

   $5x + 352y = 1$

   $352 = 5 * 70 + 2$

   Since $5 - 2 * 2 = 1$ and $352 - (5 * 70) = 2$

   $5 - [352 - (5 * 70)]^2 = 1$

   $5 - [352^2 - 2(352(5 * 70)) + (5 * 70)^2] = 1$

   $5 + 352^2 + 5(704 * 70) + (5 * 70)^2 = 1$

   $5 + 352^2 + 5(49280) - 5(24500) = 1$

   $5 + 5(49280) - 5(24500) + 352^2 = 1$

   $5 (1 + 49280 - 24500) = 1 \bmod 352$

   $5 (24781) = 1 \bmod 352$

   $d = 24781$

3. To send an encrypted message, Alice should XOR her message with a shared secret key. For Bob to decrypt the message, he should XOR the message with the shared secret key. This works because if you XOR a message with the same

key twice, the key will be nullified and the result will be just the message. In public key cryptography, the key has a secret part and a public part. If Alice wants to send Bob a message, she needs his public key. Bob's public key is published, and everyone has access to it. Alice encrypts and sends a message to Bob using the public key. Bob can then decrypt this message with the secret part of the key.

4. No, message authentication code does not preserve non-repudiation, but digital signatures can. Since the message authentication code uses a secret key which is shared between sender and receiver, a receiver can get messages with the key but it doesn't ensure they are receiving an unmodified message. Digital signatures use both private and public key. The sender encrypts the message using the private key, and it is decrypted with the receiver's public asymmetric key-pair. This enables receivers to verify a message using the public key.
5. Consider Diffie-Hellman protocol.
    a. The Diffie-Hellman protocol is used for generating a shared private key between two users to allow for exchange of messages on an insecure channel.
    b. Given p = 13, g = 4, SA = 3, and SB = 5. Compute TA, TB, and the shared key k

        $TA = g^a \bmod p$

        $= 4^3 \bmod 13$

        $= 12$

TB = $g^b$ mod p

= $4^5$ mod 13

= 10

K = $TB^a$ mod p = $10^3$ mod 13

= $TA^b$ mod p = $12^5$ mod 13 = 12

c. Diffie-Hellman protocol is vulnerable to the Man-in-The-Middle attack because the there is no key authentication when the keys are exchanged between users.

6.

a. $m_2^1$ mod $n$

   i. $(m_2^1)^d$ mod $n$ = $(m_2^d)^1$ mod $n$ = $(m_2^d$ mod $n)^1$ mod n

      = $(m_2^d$ mod $n)$ mod n

b. $m_2^2$ mod $n$

   **i.** $(m_2^2)^d$ mod $n$ = $(m_2^d)^2$ mod $n$ = $(m_2^d$ mod $n)^2$ mod n.

      Raise signature of $m_2$ to the 2nd power mod n.

c. $m_1 \cdot m_2$ mod $n$

   i. $(m_1 \cdot m_2)^d$ mod $n$ = $m_1^d \cdot m_2^d$ mod n = [$(m_1^d$ mod n)$\cdot(m_2^d$ mod n)] mod n

      Multiply Fred's two signatures mod n.

7.

a. Server should send challenge initially so the client will have to to respond.

b. Have the sender and receiver do different things. Different keys and different challenges.

8. There are flaws. Since the protocol is not symmetric, Alice can’t verify Bob’s identity.