Student Name: Wenhao Lu
Student number : S3810097

COSC2536/2537 Security in Computing and Information Technology

Q1. Encryption using Public-Key Cryptography

A) my student number is S3810097, so M=3810097

Bob pick two prime numbers p = 3919 and q = 2789.

Calculate n = p * q = 3919 * 2789 = 10930091

Calculate n' = (p-1) * (q-1) = 3918 * 2788 = 10923384

Bob choose a prime number e = 7, gcd(7, 10923384) = 1. Let's pick e=7

Public key is (10930091,7)

Generate private key de = 1 mod n'

d * 7 = 1 mod 10923384

d= 7 ^ -1 mod 10923384 = 3120967

Alice encrypt message ***M***

C = M ^e mod n

C = 3810097 ^ 7 mod 10930091 = 3415850

Bob decrypt the encrypted message ***C***

M = C ^d mod n = 3415850 ^ 3120967 mod 10930091 = 3810097

B) my student number is S3810097, so M=3810097

Bob choose : p = 4000159, g = 56, and x = 1634

Bob calculate y =g^x mod p = 56 ^1634 mod 4000159= 1954903

Bob sends public key p = 4000159, g = 56, and y = 1954903 to Alice

Alice chooses a random number ***r = 2317 and calculates***

K = y^r mod p = 1954903 ^ 2317 mod 4000159 = 793094

Alice calculate c1 and c2 as follows:

C1 = g^r mod p = 56 ^ 2317 mod 4000159 = 2281325

C2 = m * k mod p = 3810097 * 793094 mod 4000159 = 959769

Alice sends c1 and c2 to Bob

Bob calculates k and modular multiplicative increase using extended Euclidean Algorithm

K = c1 ^x mod p = 2281325 ^ 1634 mod 4000159 = 793094

K ^ -1 = 793094 ^ -1 mod 4000159 = 961957

Bob decrypts the encrypted message

M = k ^ -1*c2 mod p = 961957 * 959769 mod 4000159 = 3810097

Q2. Digital Signature using Public-Key Cryptography

my student number is S3810097, so M=3810097

Alice picks two prime numbers p = 4373 and q = 3407

Alice calculate n = p * q = 4373 * 3407 = 14898811

Calculate n’ = (p-1) * (q-1) = 4372 * 3406 = 14891032

Alice choose a prime number e = 19, gcd(19, 14891032) = 1. Let’s pick e=7

Public key is (14891032,19)

Alice sends the public key to Bob

Alice generate private key to sign the message m = 3810097

Let d be the private key , de = 1 mod n’

d * 19 = 1 mod 14891032 = 13323555

d = 13323555

Signing by Alice

Alice signs the message using private key d = 13323555 as follows:

s= m^d mod n = 3810097 ^ 13323555 mod 14898811 = 13013130

Alice sends (***3810097,13013130***) to Bob

Verification by Bob

Bob verifies using public key (14891032,19) as follows:

M’ = s^e mod n = 13013130 ^ 19 mod 14898811 = 3810097

Verify successfully

Q3. Privacy-Preserving Computation using Public-Key Cryptography

Q1 my student number is S3810097, so m1 = 7, m2 = 9

Bob chooses two prime numbers: p = 79 and q = 83

Bob calculates ***n = 79 * 83 = 6557***
Bob calculates: ***$\varphi(n) = (p-1) \times (q-1) = (79-1) \times (83-1) = 6396$***

Bob chooses: $e = 19$
Bob calculates: $d = e^{1}\ mod\ \varphi(n) = 19^{-1}\ mod\ 6396 = 3703$
Bob's public key: ***(n,e) = (6557, 19)***
Bob sends public key ***(n,e)*** to Alice.
Sender:
Alice calculates two ciphertexts for two messages, M_1 and M_2, as follows:

C1 = Me modn=7^19 mod 6557 =1640

C 2= Me modn=9^19 mod 6557 =3028

Alice sends (C_1, C_2) to the cloud for multiplication.

Cloud:

The cloud calculates: $C = C_1 . C_2$ = 1640 * 3028 = 4965920 The cloud sends ***C*** to Bob.

Receiver:

Bob decrypts the message as follows:
M= C^d *modn*= 4965920 ^ 3703 *mod* 6557 = 63 **The result of the multiplication is M = 63**

Q2 my student number is S3810097, so m1 = 7, m2 = 9

Receiver generates: p = 5081, g = 93

Secret key x = 106

Receiver computes: ***y = gx mod p = 93 ^ 106 mod 5081 = 4543***

Receiver sends: p = 5081, g = 93, and y = *4543* to sender

Sender chooses two random numbers : r1 = 79 and r2 = 94

Sender calculates: ***k1 = yr1 mod p = 4543 ^ 79 mod 5081 = 9***

k2 = yr2 modp= 4543 ^ 94 mod 5081 = 963

Sender calculates C_1 and C_2two messages $m_1 = 7$ and $m_2 = 9$ as follows:

C11 = gr1 mod p = 93 ^ 79 mod 5081 = 1328

C12 =(m1 .k1)modp=(7*9) mod 5081=63

C21 = gr2 mod p = 93 ^ 94 mod 5081 = 2224

C22 =(m2 .k2)modp=(9*963) mod 5081=3586

Sender sends: (C_{11}, C_{12}) and (C_{21}, C_{22}) to cloud server. Cloud server computes ***A*** and ***B*** as follows:

A = (C11. C21) mod p = (1328 * 2224) mod 5081 = 1411

B = (C12. C22) mod p = (63 * 3586) mod 5081 = 2354

Cloud server sends ***A*** and ***B*** to receiver.
Receiver computes the result ***M = m1 * m2*** as follows:

M= B mod p / a ^x mod p = 2354 mod 5081 / 1411 ^ 106 mod 5081 = 2354 mod 5081 / 3586 mod 5081 = 63

The final result is: ***M = 63.***

Q4 Designing a Secure Authentication Protocol

Answer: two nonce: Ra and Rb are used to authenticate both bob and Alice .

Problem: insecure . Man-in-middle attack is possible

Trudy send the message "alice" and ra to bob

Then bob reply Rb and e (Ra,Kab)

Trudy does not know the Kab. Then he create a new Session

Trudy send the message "Alice" and Rb

Then bob reply Rc, and e (Rb,Kab), trudy get the information and back to Session1 send e (Rb,Kab) to bob in order to convince Bob that she is Alice.