Name: Priyanka, student-id: 20179, Week-3, HW2

Part-1

A. Key Generation

Key Generation	Questions related to Key Generation

Item	Alice	Bob
Assumption	d = 7, G=5	d = 3, G=5
Public Key	Step 1-B PU_{Alice} = ??	Step 1-A PU_{Bob} = ??
Private Key	Step 1-B PR_{Alice} = ??	Step 1-A PR_{Bob} = ??

- Does Eve know
- Bob's public key P_{Bob}? ??
- Bob's private key S_{Bob}? ??
- Alice's public key P_{Alice}? ??
- Alice's private key S_{Alice}? ??
- Does Alice know
- Bob's public key P_{Bob}? ??
- Bob's private key S_{Bob}? ??
- Does Bob know
- Alice's public key P_{Alice}? ??
- Alice's private key S_{Alice}? ??
- How many keys are required for N people to communicate using Asymmetric Key Cryptography? ??

Solution:

A. Key Generation

Key Generation	Questions related to Key Generation

Item	Alice	Bob
Assumption	d = 7, G=5	d = 3, G=5
Public Key	Step 1-B PU_{Alice} ➔ 35	Step 1-A PU_{Bob} ➔15
Private Key	Step 1-B PR_{Alice} ➔ 7	Step 1-A PR_{Bob} ➔3

- Does Eve know
- Bob's public key P_{Bob} ➔ yes
- Bob's private key S_{Bob} ➔no
- Alice's public key P_{Alice} ➔yes
- Alice's private key S_{Alice} ➔no
- Does Alice know
- Bob's public key P_{Bob} ➔yes
- Bob's private key S_{Bob} ➔no
- Does Bob know
- Alice's public key P_{Alice} ➔yes
- Alice's private key S_{Alice} ➔no
- How many keys are required for N people to communicate using

	Asymmetric Key Cryptography ➔2N

B.

Confidentiality

Alice sends the message (the number 11) to Bob

Alice	**Bob**
Step 2-A: Alice uses Bob's public key P_{Bob} to encrypt the message: 11 Question: ▪ What are the values of C1 and C2? C1=K*G C1 =PRA * G We have D=7, G=5 Q=D*G(Q=public key, d=private, G= base point) Q=7*5=35 Q=35 C1=35 C2=M+K+Q C2=M + PRA * PUB C2=11+7*15 C2=11+105 C2=116	Step 4-A: Bob uses his private key PR_{Bob} (i.e, secret key S_{Bob}) to decrypt the cipher text and retrieve the message (the number 11). Questrion? ○ What is the value of msg' ? Value ➔11 ==> Proof Msg'=C2-d*C1 Msg'= (M + PRA * PUB) - PRB * PUA Msg'= (11+7*15)- 3*35 Msg'= 11+105-105 Msg'=11+0 Msg'=11 So, msg=msg' ○ Instead of msg, why would Bob receive msg'? Answer: Bob receives msg' because during the encryption process, the original message M is transformed into the ciphertext C2, and the decryption process recovers the message as msg'. ○ Can Eve read the original message on Step 3-A. Answer: No, because Eve does not have access to the private keys needed to decrypt the message.

	○ Can **Confidentiality** gurantee that Bob receives the original message sent from Alice? Answer: Yes, if the encryption is performed correctly, confidentiality ensures that only Bob can decrypt the message ○ Can **Confidentiality** gurantee that Bob knows that someone has modified Alice's message? Answer: No, confidentiality alone does not verify integrity, alice needs hash or digital signature

Authentication/integrity/non-repudaiation

Alice	**Bob**
1. Step 2-B1: Alice calculates the HASH of the message (the number 11). ▪ Assuming the MD function is message mod 3 = msg % 3 ▪ Questrion? 2. What is the value of HASH? **Answer: HASH=11MOD=2** **Value of hash=2** 3. Can Eve find the message from the HASH? **Answer: No**, the HASH is a one-way function, and HASH does not allow Eve to retrieve the original message. 4. Step 2-B2: Alice calculates the digital signature by encrypting the HASH with her private key PR_{Alice} (= secret key S_{Alice}).	1. Step 4-B: Bob finds HASH' from msg' • Again, assuming the MD function is message mod 3 = msg % 3 ▪ Questrion? • What is the value of HASH'? **Answer:** Bob retrieve msg'=11 Hash'=Msg'mod3 Hash'=11 Mod 3=2 Hash'=2 2. Step 4-C: Bob decrypts the digital signature with Alice's public key P_{Alice} and find HASH. • Questrion? • What is the value of HASH? **Answer:** Hash= C2-D_{bob} *C1 Hash= 107- 3* 15 Hash= 107-25 **Hash= 82**

Question:

5. What are the values of C1 and C2?

Answer: C1=K*G

C1=3*5=15

C1=15

C2= hash+k*PU_{alice}

C2= 2+ 3*35= 107

C2=107

6. Can Eve find the HASH from {HASH}S_{Alice} on Step 3-B?

Answer: **No**, if properly encrypted, Eve cannot find the HASH without Alice's private key.

3. Step 4-D: Compare HASH and HASH'
    - Questrion?

- Does HASH=HASH'?

Answer: Hash=2

Hash'=2

Hash=Hash'

- What conclusion can be reached if
- HASH = HAHS'

Answer: If they are equal, it means the message is correct, and Bob can confirm that it was not modified.

- HASH != HAHS'

Answer: if they are not equal, it indicates that the message was modified during transmission.

- Can Authentication/Integrity/Non-repudaiation gurantee that Bob receives the original message sent from Alice?

Answer: Yes, provided that the hashing and signature mechanisms are properly implemented

- Can Authentication/Integrity/Non-repudaiation gurantee that Bob knows that someone has modified Alice's message?

Answer: **Yes**, if the HASH values differ, it indicates modified.

- Can Authentication/Integrity/Non-repudaiation & Confidentiality gurantee that Bob receives the message sent from Alice?

Answer: yes, confidentiality protects the message while integrity ensures that it is the correct message.

- Can Authentication/Integrity/Non-repudaiation & Confidentiality gurantee that Bob knows that someone has modified Alice's message?

Answer: Yes, the combination ensures both the message's confidentiality and integrity checks.