Please copy the following tables to your answer papers and replace the ?? with your answers.

```
What Alice knows & does    | What Eve (the public)     | What Bob
                           | knows and sees            | knows and does
---------------------------+---------------------------+------------------
--
        P_Bob (1-A)        | P_Bob                     | P_Bob (1-A)
        MD                 | MD                        |   S_Bob
        P_Alice            | P_Alice                   | MD
  (1-B) S_Alice            |                           |  P_Alice
---------------------------+---------------------------+------------------
--
    (2-A)                  |                           |          (4-A)
    +P_Bob                 | (3-A)                     |         -S_Bob
msg ------> {msg}P_Bob --------> {/////}P_Bob --------> {msg}P_Bob -->
msg'
 |                         |                           |
|
 | MD (2-B1)               |                           |
|
 v                         |                           |           (4-B)
| MD
HASH                       |                           |
V
 |                         |                           |
HASH'
 |+S_Alice                 | (3-B)                     |
 +-------> {HASH}S_Alice--------> {HASH}S_Alice -----------> {HASH}S_Alice
            (2-B2)         |                           |          |
                           |                           |     (4-C)|-P_Alice
                           |                           |          V
                           |                           |         HASH
                           |                           |
                           |                           | Does
HASH=HASH'?
                           |                           |        (4-D)
```

A. Key generation

Key Generation	Questions related to Key Generation
<table><tr><th>Item</th><th>Alice</th><th>Bob</th></tr><tr><td>**Assumption**</td><td>d = 7, G=5</td><td>d = 3, G=5</td></tr><tr><td>**Public Key**</td><td>Step 1-B PU_{Alice} = ??</td><td>Step 1-A PU_{Bob} = ??</td></tr><tr><td>**Private Key**</td><td>Step 1-B PR_{Alice} = ??</td><td>Step 1-A PR_{Bob} = ??</td></tr></table>	- 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? ??

B. Confidentiality & Authentication

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: Question: ▪ What are the values of C1 and C2? ??	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' ? ??

	==> Proof ?? - Instead of msg, why would Bob receive msg'? ?? - Can Eve read the original message on Step 3-A. ?? - Can **Confidentiality** gurantee that Bob receives the original message sent from Alice? ?? - Can **Confidentiality** gurantee that Bob knows that someone has modified Alice's message? ??

Authentication

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? ◦ What is the value of HASH? ??	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'? ?? 2. Step 4-C: Bob decrypts the digital signature with Alice's public key P_{Alice} and find HASH. ▪ Questrion?

<table>
<tr>
<td>

- Can Eve find the message from the HASH? ??

2. Step 2-B2: Alice calculates the digital signature by encrypting the HASH with her private key PR_{Alice} (= secret key S_{Alice}).

Question:

- What are the values of C1 and C2?

  ??

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

</td>
<td>

- What is the value of HASH?

  ??

3. Step 4-D: Compare HASH and HASH'
   - Questrion?
     - Does HASH=HASH'? ??
     - What conclusion can be reached if
       - HASH = HAHS' ??
       - HASH != HAHS' ??
     - Can Authentication gurantee that Bob receives the original message sent from Alice? ??
     - Can Authentication gurantee that Bob knows that someone has modified Alice's message? ??

</td>
</tr>
</table>

	- Can Authentication & Confidentiality gurantee that Bob receives the message sent from Alice? ?? - Can Authentication & Confidentiality gurantee that Bob knows that someone has modified Alice's message? ??

Ans:

Key Generation	Questions related to Key Generation
<table><tr><th>Item</th><th>Alice</th><th>Bob</th></tr><tr><td>**Assumption**</td><td>d = 7, G=5</td><td>d = 3, G=5</td></tr><tr><td>**Public Key**</td><td>Step 1-B PU_{Alice} = 35</td><td>Step 1-A PU_{Bob} = 15</td></tr><tr><td>**Private Key**</td><td>Step 1-B PR_{Alice} = 7</td><td>Step 1-A PR_{Bob} = 3</td></tr></table>	- 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 keys are required

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: Question: - What are the values of C1 and C2? C1 = K*G=7*5=35 C2= M+K*Q= 11+7*15=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' ? msg' = C2-d*C1 = 116-3*35=11 ==> Proof

	msg'=msg ◦ Instead of msg, why would Bob receive msg'? because Bob uses his Private Key to decrypting and get msg ◦ Can Eve read the original message on Step 3-A. no, because this step need Bob's Private Key to decrypting, Alice don't have Bob's Private Key ◦ Can **Confidentiality** gurantee that Bob receives the original message sent from Alice? Yes ◦ Can **Confidentiality** gurantee that Bob knows that someone has modified Alice's message? No

Authentication

Alice	Bob
3. Step 2-B1: Alice calculates the HASH of the message (the number 11). ▪ Assuming the MD function is message mod 3 = msg % 3 ▪ Questrion? ◦ What is the value of HASH? HASH=11%3=2 ◦ Can Eve find the message from the HASH? No, because the HASH is one way	4. 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'? HASH'=2 5. 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? HASH=2

4. Step 2-B2: Alice calculates the digital signature by encrypting the HASH with her private key PR_{Alice} (= secret key S_{Alice}). Question: ▪ What are the values of C1 and C2? C1=7*5=35 C2=2+7*15=107 ▪ Can Eve find the HASH from $\{HASH\}S_{Alice}$ on Step 3-B? Yes, because she know the Alice's Public Key	6. Step 4-D: Compare HASH and HASH' ▪ Questrion? ○ Does HASH=HASH'? yes ○ What conclusion can be reached if ▪ HASH = HAHS' If Hash = Hash', then means there is no one modified the original message and can be sure message was sent from Alice. ▪ HASH != HAHS' If Hash != Hash', then means someone may modified the original message or this message may not sent from Alice ○ Can Authentication gurantee that Bob receives the original message sent from Alice? Yes ○ Can Authentication gurantee that Bob knows that someone has modified Alice's message? no

	◦ Can Authentication & Confidentiality gurantee that Bob receives the message sent from Alice? yes ◦ Can Authentication & Confidentiality gurantee that Bob knows that someone has modified Alice's message? yes