1.

1. a. $p = 11$. $g = 13$

$T_A = g^{SA} \bmod p$ $(SA = 2)$

$= 13^2 \bmod 11$

$= 13 \times 13 \bmod 11$

$= 2 \times 2 \bmod 11$

$= 4$

$T_B = g^{SB} \bmod p$ $(SB = 3)$

$= 13 \times 13 \times 13 \bmod 11$

$= 2 \times 2 \times 2 \bmod 11$

$= 8$

$T_B^{SA} \bmod p$

$= 8^2 \bmod 11$

$= 8 \times 8 \bmod 11$

$= 3 \times 3 \bmod 11$

$= 9$.

$T_A^{SB} \bmod p$

$= 4^3 \bmod 11$

$= (4 \times 4 \bmod 11 * 4 \bmod 11) \bmod 11$

$= 9$

∴ 9 is the secret key

b) $p = 7$. $g = 17$

$T_A = g^{SA} \bmod p$ $(SA = 2)$

$= 17^2 \bmod 7$.

$= (17 \bmod 7 * 17 \bmod 7) \bmod 7$

$= (3 \times 3) \bmod 7$

$= 2$.

$T_B = g^{SB} \bmod p$ $(SB = 3)$

$= 17^3 \bmod 7$.

$= (17 \bmod 7 * 17 \bmod 7 * 17 \bmod 7) \bmod 7$

$= 6$.

$T_B^{SA} \bmod p$

$= 6^2 \bmod 7$

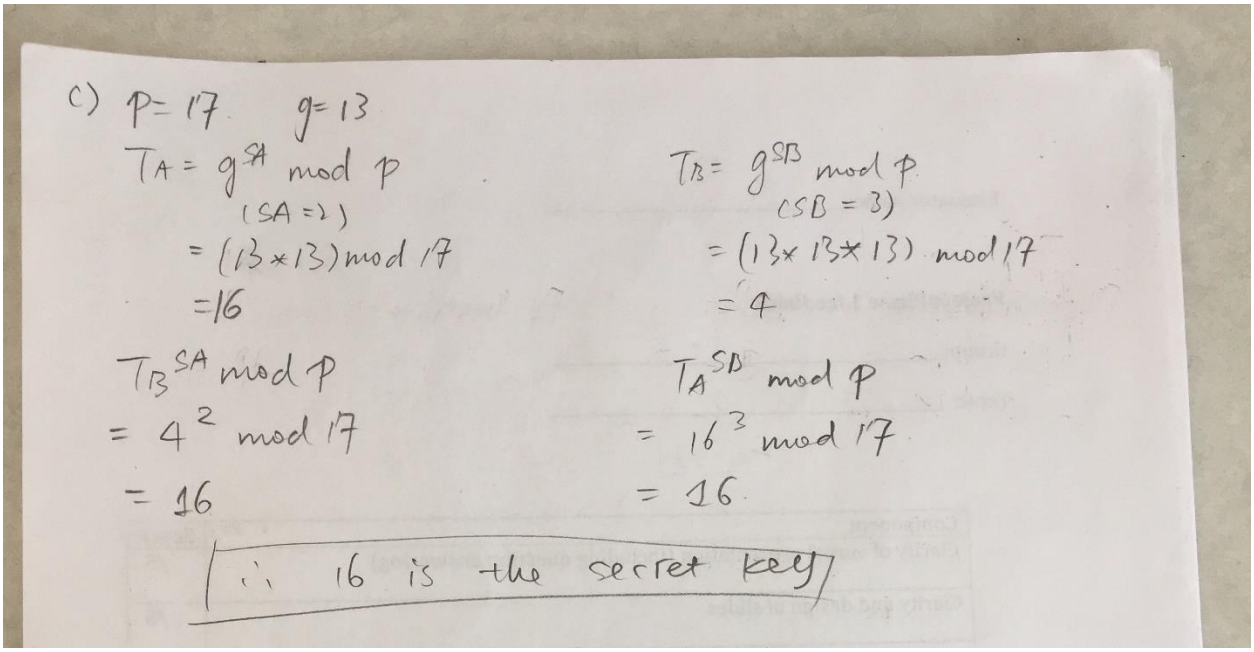
$= 1$

$T_A^{SB} \bmod p$

$= 2^3 \bmod 7$

$= 1$.

∴ 1 is the secret key



2. Sample output

```
============== RESTART: C:/Users/zehao/Desktop/6708/ass4/q2.py ==============
=
Please input the p:
11
Please input the g:
13
random key of Alice(SA) is 70198
random key of Bob(SB) is 80368
The secret key is 5
>>>
============== RESTART: C:/Users/zehao/Desktop/6708/ass4/q2.py ==============
=
Please input the p:
7
Please input the g:
17
random key of Alice(SA) is 8465
random key of Bob(SB) is 63279
The secret key is 6
```

3. Note:

- Payload means the payload is encrypted
- Payload means it is authenticated
- The original datagram is

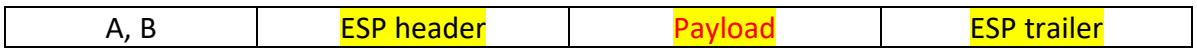
A, B	Payload

a) ESP transport mode only from end to end

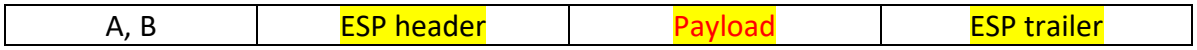
I. At A

A, B	Payload

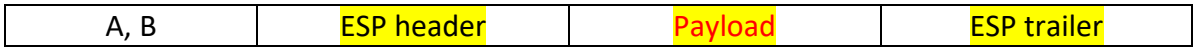
II. A to G1



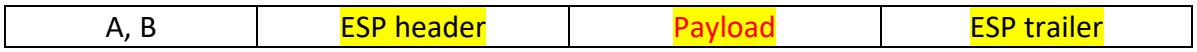
III. G1 to G3



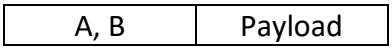
IV. G3 to G2



V. G2 to B

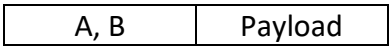


VI. At B

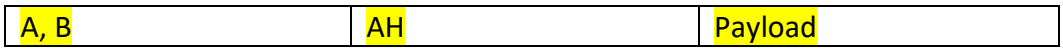


b) AH transport from A to B, ESP tunnel from firewall G1 to firewall G2

I. At A



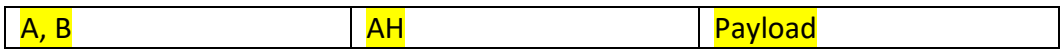
II. A to G1



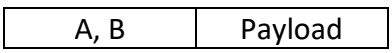
III. G1 to G3

IV. G3 to G2

V. G2 to B

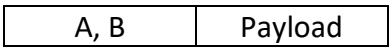


VI. At B

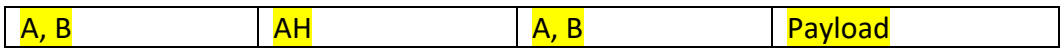


c) AH tunnel from A to B, ESP transport from firewall G1 to firewall G3

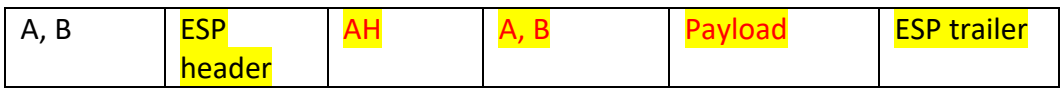
I. At A



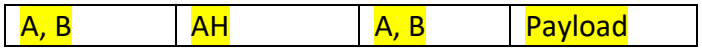
II. A to G1



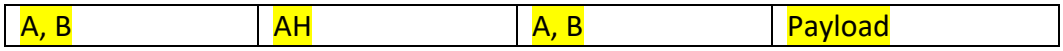
III. G1 to G3



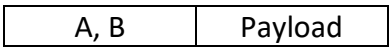
IV. G3 to G2



V. G2 to B

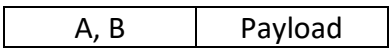


VI. At B



d) ESP tunnel from G3 to G2, and AH tunnel from G2 to B

I. At A



II. A to G1

A, B	Payload

III. G1 to G3

A, B	Payload

IV. G3 to G2

G3, G2	ESP header	A, B	Payload	ESP trailer

V. G2 to B

G2, B	AH	A, B	Payload

VI. At B

A, B	Payload

4.

a) Brute-Force attack: This attack can be prevented by enlarge the size of key of the encryption algorithm. Such as 3DES with 168 bits key, AES with 256 bits key, and IDEA with 128 bits key, etc.

b) Replay attack: The sequence number is used to prevent replay attack. The sequence number exists in both authentication header and encapsulating security payload. For example, the user sends a number of packets with sequence number, the receiver will check if the packet has been sent previously or not so that the receiver can decide whether accept the packet or not;

c) Man in the middle attack: The internet key exchange(IKE) can prevent the man in the middle attack. In the internet key exchange, there is a security association(SA) with two phases. In the first phase, sender and receiver negotiate SAs, use the Diffie Hellman to generate the master key. Finally, the sender and receiver authenticate each other by exchanging the digital signatures and certificates. In the second phase, they do another Diffie Hellman exchange using the encrypted packets and protected by digital signatures and generate the secret session key. Now, data can be transferred using the secret session key. The secret session key is refreshed every few minutes. In this process, the Diffie hellman algorithm makes the key is difficult for others to get it. Besides, the authentication keeps the attacker away from the user since there is digital signatures and certification. And the secret session key will be refreshed every few minutes, although the attacker gets the temporarily one, it still cannot attack the server or client continuously.

d) IP spoofing: During the transmission, there are authentications between sender and receivers. The authentications including digital signatures and certificates. Once they are authenticated, the sender and receiver begin to encrypt the message.

e) SYN flooding: During the transmission, the sender and receiver are authenticated first, which means they authenticate the IP address to each other so that there is no attacker or invalid information. If the information cannot be authenticated, the host will not be allowed to do the next step, therefore, the host will not wait for the next message.