Assignment 3

Name: Zewen Wang B#: B00756586

Q1 :

1. p = 11, g = 13
   - Assume: SA = 6, SB = 4
   - TA = g^{SA} mod p = 13^6 mod 11 = (13*13*13*13*13*13) mod 11 = 2^6 mod 11 = 9
     TB = g^{SB} mod p = 13^4 mod 11 = 2^4 mod 11 = 16 mod 11 = 5
   - TA <--> TB
     TB^{SA} mod p = 5^6 mod 11 = (3*3*3) mod 11 = 27 mod 11 = 5
     TA^{SB} mod p = 9^4 mod 11 = (81*81) mod 11 = 16 mod 11 = 5
   - 5 is the secret key.

2. p = 7, g = 17
   - Assume: SA = 7, SB = 6
   - TA = g^{SA} mod p = 17^7 mod 7 = (17*17*17*17*17*17*17) mod 7 = 3^7 mod 7 = 3
     TB = g^{SB} mod p = 17^6 mod 7 = 3^6 mod 7 = 8 mod 7 = 1
   - TA <--> TB
     TB^{SA} mod p = 1^7 mod 7 = (2*2*2*3) mod 7 = 1
     TA^{SB} mod p = 3^6 mod 7 = 2^6mod 7 = 64 mod 7 = 1
   - 1 is the secret key.

3. p = 17, g = 13
   - Assume: SA = 4, SB = 7
   - TA = g^{SA} mod p = 13^4 mod 17 = (13*13*13*13) mod 17 = (16*16) mod 17 = 1
     TB = g^{SB} mod p = 13^7 mod 17 = (16^3*13) mod 17 = 4
   - TA <--> TB
     TB^{SA} mod p = 4^4 mod 17 = (13*4) mod 17 = 1
     TA^{SB} mod p = 1^4 mod 17 = 1
   - 1 is the secret key.

Q2: I use python3 to code and the source code can be seen from the file ”DiffieH”.
The sample outputs for question 1 are shown below:

```
T909C:Assignment4_B00756586 wangzewen$ python3 DiffieH.py
Please enter p : 11
Please enter g : 13
The secret key SA is  2
The secret key SB is  358
9  is the secret key.
T909C:Assignment4_B00756586 wangzewen$ python3 DiffieH.py
Please enter p : 7
Please enter g : 17
The secret key SA is  120
The secret key SB is  24
1  is the secret key.
T909C:Assignment4_B00756586 wangzewen$ python3 DiffieH.py
Please enter p : 17
Please enter g : 13
The secret key SA is  623
The secret key SB is  438
16  is the secret key.
```

Q3:

Note: The shaded area is the encryption part and "a" means authentication part.

a)

(1) original datagram:

A, B	Payload

(2) A—>G1 segment:

A, B	ESP Header	Payload	ESP Trailer

|<----------a---------->|

(3) G1—>G3 segment:

A, B	ESP Header	Payload	ESP Trailer

|<----------a---------->|

(4) G3—>G2 segment:

A, B	ESP Header	Payload	ESP Trailer

|<----------a---------->|

(5) G2—>B segment:

A, B	ESP Header	Payload	ESP Trailer

|<----------a---------->|

(6) At B:

A, B	Payload

b)

(1) original datagram:

A, B	Payload

(2) A—>G1 segment:

A, B	AH	Payload

|<----------a---------->|

(3) G1—>G3 segment:

G1, G2	ESP Header	A, B	AH	Payload	ESP Trailer

|<----------a---------->|

(4) G3—>G2 segment:

G1, G2	ESP Header	A, B	AH	Payload	ESP Trailer

|<----------a---------->|

(5) G2—>B segment:

A, B	AH	Payload

|<----------a---------->|

(6) At B:

A, B	Payload

c)

(1) original datagram:

A, B	Payload

(2) A—>G1 segment:

A, B	AH	A, B	Payload

|<----------a---------->|

(3) G1—>G3 segment:

A, B	ESP Header	AH	A, B	Payload	ESP trailer

|<----------a---------->|

(4) G3—>G2 segment:

A, B	AH	A, B	Payload

|<----------a---------->|

(5) G2—>B segment:

A, B	AH	A, B	Payload

|<----------a---------->|

(6) At B:

A, B	Payload

d)

(1) original datagram:

A, B	Payload

(2) A—>G1 segment:

A, B	Payload

(3) G1—>G3 segment:

A, B	Payload

(4) G3—>G2 segment:

G3, G2	ESP Header	A, B	Payload	ESP Trailer

|<----------a---------->|

(5) G2—>B segment:

G2, B	AH	A, B	Payload

|<----------a---------->|

(6) At B:

A, B	Payload

Q4:

a. Brute-Force Attack:

IPSec provides many encryption algorithms such as AES, RC4, 3DES and other encryption algorithms. These encryption algorithms have long key length, which makes Brute-Force Attack extremely hard to launch.

b. Replay Attack:

IPSec consists of three important components, including authentication header, encapsulating security payload and internet key exchange. These components can mitigate Replay Attack by using generated sequence numbers which are stored in a table. If an attack duplicates encrypted packets and tries to launch the replay attack, the receiver who keeps track of packets will compare the sequence number of these packets with those stored in the table. If it is found that the number has already stored in the table, this may occur the replay attack and the packet will be discarded.

c. Man-in-the-middle Attack:

Among the three components of IPSec mentioned above, the Internet Key Exchange(IKE) protocol provides the security of key exchange during communications which can mitigate Man-in-the-middle Attack. Besides, this attack can also be prevented by authentication.

d. IP Spoofing:

Negotiating an IPSec connection requires mutual authentication, which is a way to prove the identity of the entity behind the IP address. All communications are cryptographically sound, so it must go through the mutual authentication phase. [1] Therefore IP Spoofing is countered.

e. SYN Flooding:

The IPSec Security Association creation requires authentication, the current form of SYN flooding attacks which use a forged source IP address in the SYN packets are precluded. If the attacker uses a real source IP address to launch the attack, then the attacker’s identity is known and provable, in that case, one can add packet filters. [2]

Reference:

[1] How does IPSec protect against IP spoofing? (n.d.). Retrieved April 03, 2017, from https://security.stackexchange.com/questions/46340/how-does-ipsec-protect-against-ip-spoofing
[2] Re: transport vs network and ipsec syn. (n.d.). Retrieved April 03, 2017, from http://www.sandelman.ottawa.on.ca/ipsec/1997/03/msg00033.html