Question 1

1) prime number $p, q = 7, 11$

secret message $= 6$.

modulus, $n = p \times q = 77$.

totion function, $\phi(n) = (p-1)(q-1) = 60$

→ Calculating public key 'e':

such that $\begin{Bmatrix} 1 < e < \phi(n), \\ \gcd(e, \phi(n)) = 1 \end{Bmatrix}$

$\therefore e = 37$

public key $= \{37, 77\}$

→ Calculating private key 'd':

such that $d = \dfrac{1 + K\,\phi(n)}{n}$, where K is a random number such that 'd' is a whole number

OR

$\boxed{d \times e \bmod \phi(n) = 1}$

$d = \dfrac{1 + 93 \times 60}{77}$

$d = 73$

private key $= \{73, 77\}$

→ Message '6' encryption.

$= M^e \bmod n = 6^{37} \bmod 60 = 54$

2) prime number $p, q = 11, 13$

Modulus .= $n = p \times q = 11 \times 13 = 143$

$\phi(n) = 120$

let, 'e' be → 47.

∴ public key = $\{47, 143\}$

let 'd' be

$d * e \bmod (\phi(n)) = 1$

∴ $d = 143$

private key = $\{143, 143\}$

∴ Encrypted message is $M^e \bmod n$

$= 9^{47} \bmod 143 = \underline{\underline{81}}$

3) prime number $p, q = 17, 31$

Modulus = 527

$\phi(n) = 480$

let 'e' be → 247.

public key $\{247, 527\}$

∴ $d \cdot e \bmod \phi(n) = 1$

∴ $d = 583$

private key = $\{583, 527\}$

∴ The encrypted message '5' is.

$5^{247} \bmod 480 = \underline{365}$

Q2

a) The prime number given 'g' = 13

The primitive root given 'p' = 11

let 'A' assume values ~~E~~ 'X_A' = 6 (private key of 'A')

let B assume value 'X_B' 8 (private key of 'B').

The public key of 'A' "Y_A" is = $p^{X_A} \bmod g$

$= 11^6 \bmod 13 = 12$

The public key of B "Y_B" is = $p^{X_B} \bmod g$.

$= 11^8 \bmod 13$

$= 9.$

PROOF:-

Now A & B will exchange ~~B~~ Y_A & Y_B and ~~try to~~ decrypt it to see the message.

A sender	B receiver.
$(Y_B)^{X_A} \bmod q$	$(Y_A)^{X_B} \bmod q$
$(9)^6 \bmod 13$	$(12)^8 \bmod 13$
$= 1$	$= 1$

Q2

(b) The prime number given 'g' = 17

The primit root given 'p' = 7

Let 'A' assume a private key 'X_A' = 6

Let B assume a private key 'X_B' = 8

The public key of 'A' is 'Y_A' = $(p)^{X_A} \bmod g$ = $(7)^6 \bmod 17 = 9$

The public key of B 'Y_B' = $(p)^{X_B} \bmod g = 16$

PROOF:

A sender	B Receiver
$(Y_B)^{X_A} \bmod g$	$(Y_A)^{X_B} \bmod g$
$(16)^6 \bmod 17$	$(9)^8 \bmod 17$
1	1

Q2

c) The prime number given 'g' = 17

The primite root given 'p' = 13

~~The~~ let 'A' assume private key 'X_A' = 6

let 'B' assume private key 'X_B' = 8

The public key of A is 'Y_A' $= (p)^{X_A} \bmod g = (13)^6 \bmod 17 = 16$

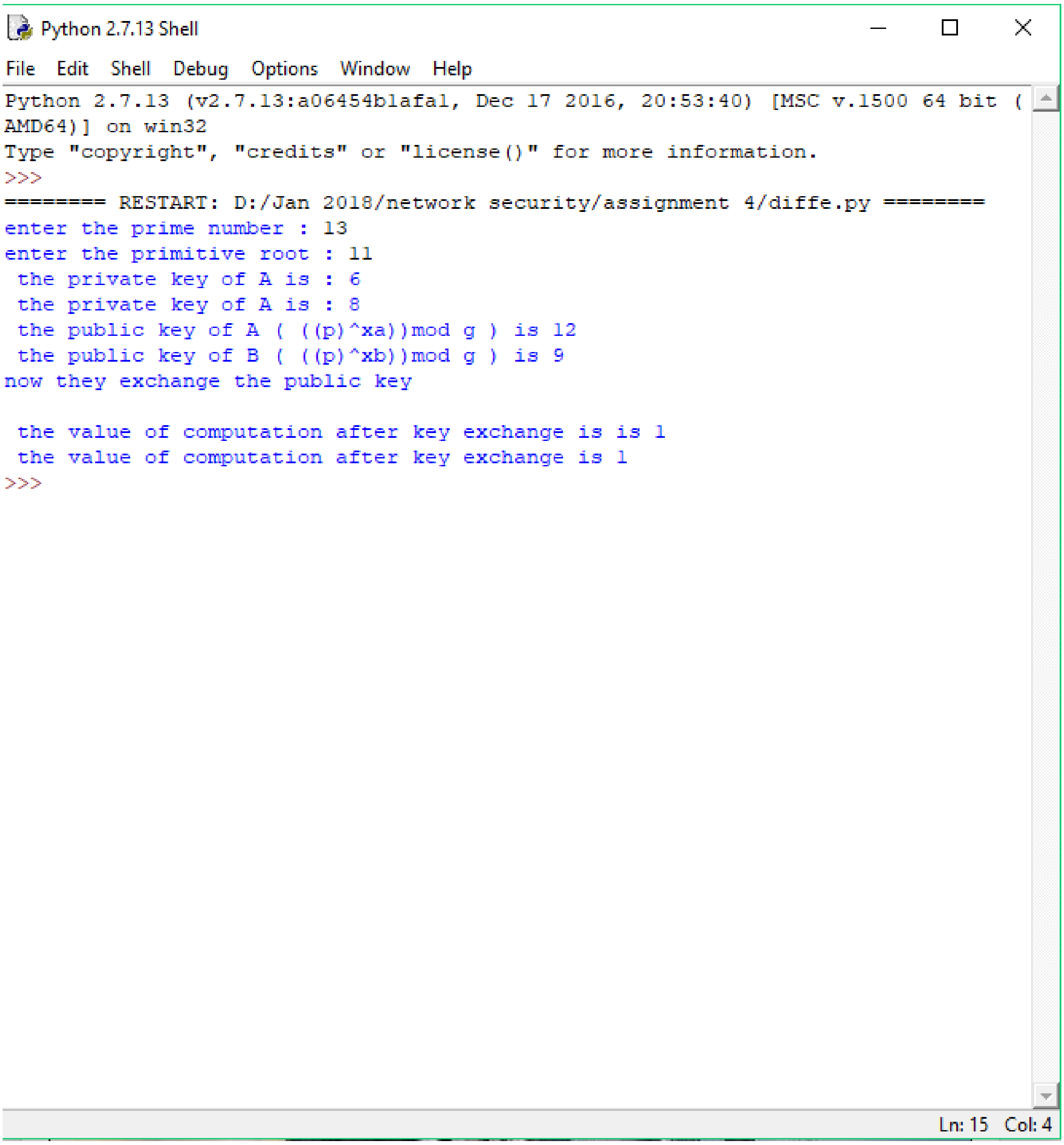
The public key of B is 'Y_B' $= (p)^{X_B} \bmod g = (13)^8 \bmod 17 = 1$

PROOF

A Sender	B Receiver.
$(Y_B)^{X_A} \bmod g$	$(Y_A)^{X_B} \bmod g$
$(1)^6 \bmod 17$	$(16)^8 \bmod 17$
$\underline{\underline{1}}$	$\underline{\underline{1}}$

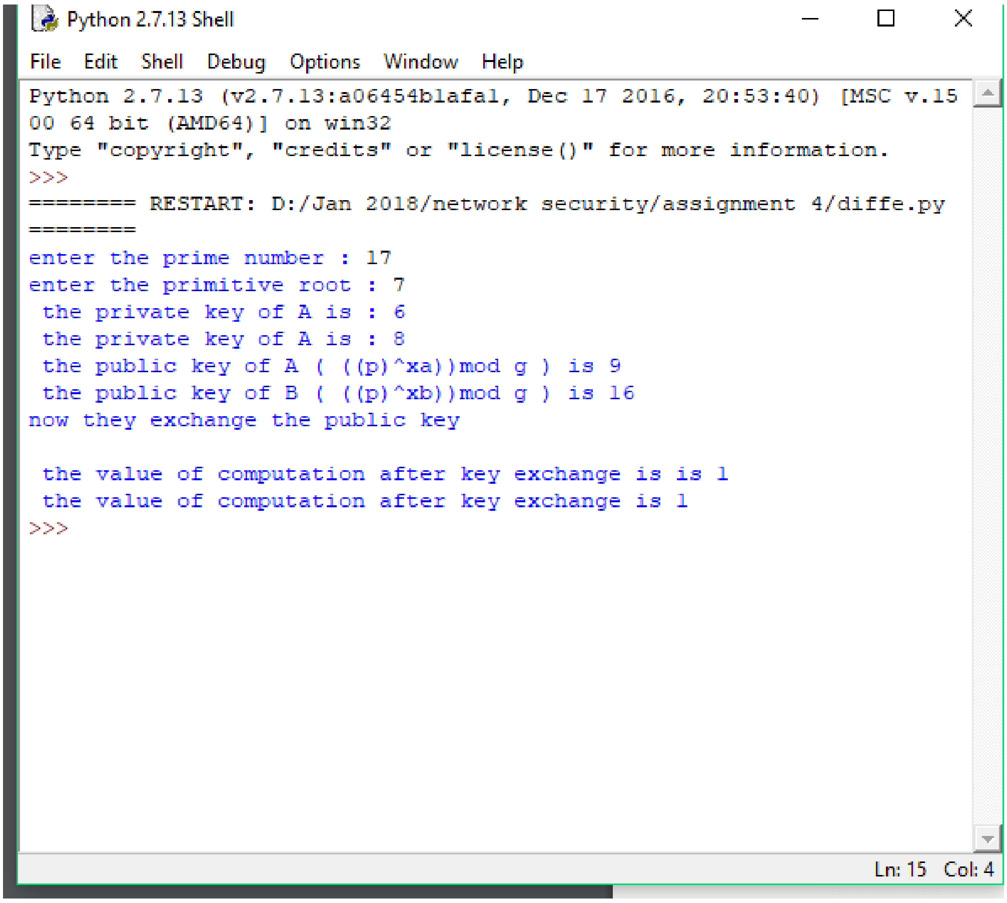
Question 3:

a.



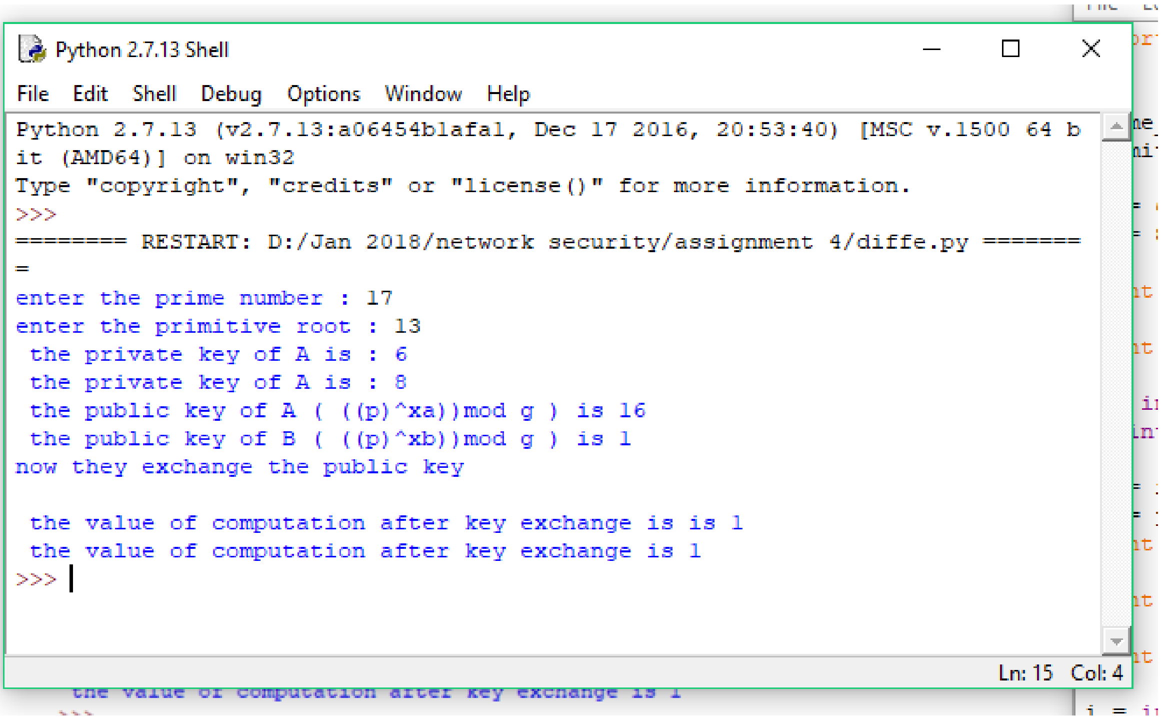
```
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40) [MSC v.1500 64 bit (
AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
======== RESTART: D:/Jan 2018/network security/assignment 4/diffe.py ========
enter the prime number : 13
enter the primitive root : 11
 the private key of A is : 6
 the private key of A is : 8
 the public key of A ( ((p)^xa))mod g ) is 12
 the public key of B ( ((p)^xb))mod g ) is 9
now they exchange the public key

 the value of computation after key exchange is is 1
 the value of computation after key exchange is 1
>>>
```

b.



```
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40) [MSC v.15
00 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
======== RESTART: D:/Jan 2018/network security/assignment 4/diffe.py
========
enter the prime number : 17
enter the primitive root : 7
 the private key of A is : 6
 the private key of A is : 8
 the public key of A ( ((p)^xa))mod g ) is 9
 the public key of B ( ((p)^xb))mod g ) is 16
now they exchange the public key

 the value of computation after key exchange is is 1
 the value of computation after key exchange is 1
>>>
```

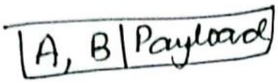
c.

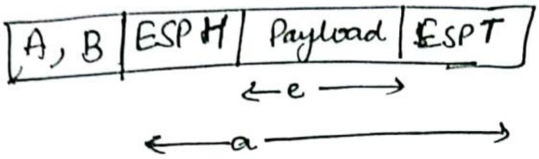


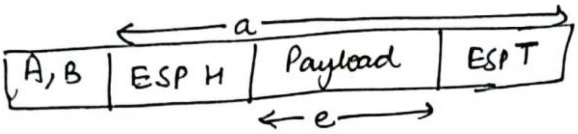
```
Python 2.7.13 (v2.7.13:a06454b1afa1, Dec 17 2016, 20:53:40) [MSC v.1500 64 b
it (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
======== RESTART: D:/Jan 2018/network security/assignment 4/diffe.py =======
=
enter the prime number : 17
enter the primitive root : 13
 the private key of A is : 6
 the private key of A is : 8
 the public key of A ( ((p)^xa))mod g ) is 16
 the public key of B ( ((p)^xb))mod g ) is 1
now they exchange the public key

 the value of computation after key exchange is is 1
 the value of computation after key exchange is 1
>>> 
```

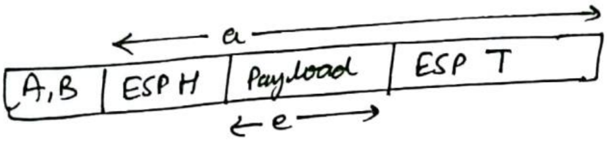
Q4.

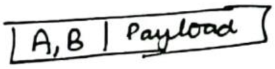
1. Esp transport from End to End.

Original datagram: 

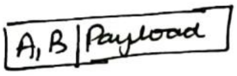
$A-G_1$: 

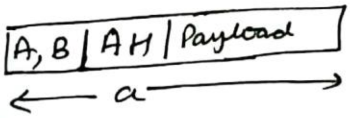
$G_1 - G_3$: 

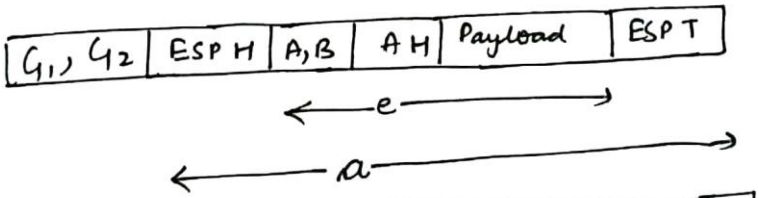
$G_3 - G_2$: 

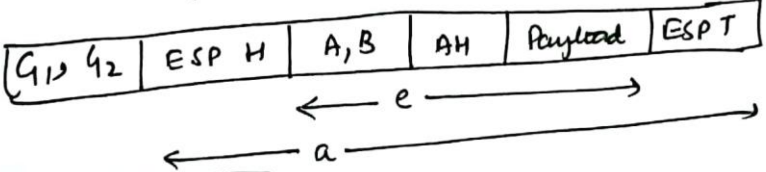
at B : 

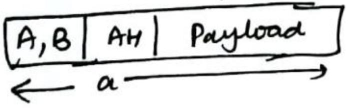
2. AH Transport from A to B, ESP tunnel betwen G_1 & G_2.

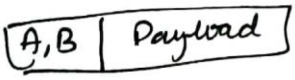
Original Datagram 

$A-G_1$:- 

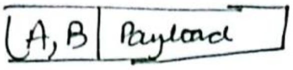
$G_1 - G_3$:- 

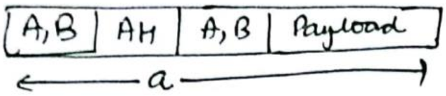
$G_3 - G_1$: 

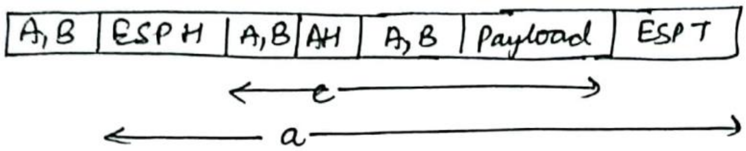
$G_1 - B$: 

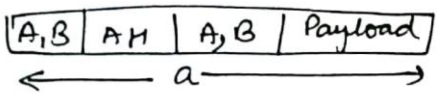
At B: 

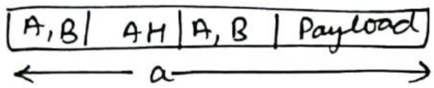
3 AH Tunnel ~~to~~ A to B, ESP transport between G_1 & G_3.

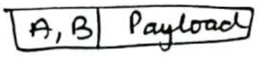
Original Datagram: 

$A-G_1$: 

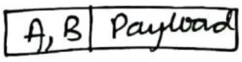
G_1-G_3: 

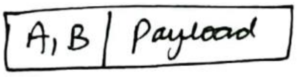
G_3-G_2: 

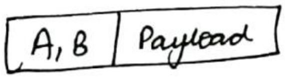
G_2-B: 

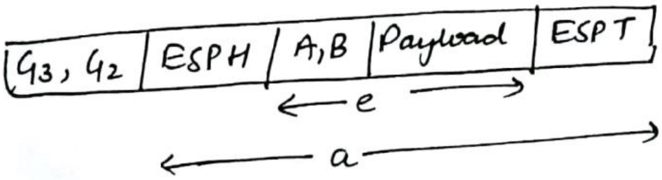
~~A~~ B: 

4. ESP tunnel from G_3 to G_2, AH tunnel from G_2 to B

Original Datagram. 

$A-G_1$: 

G_1-G_3: 

G_3-G_2: 

G_2-B: