**1.** encrypt letter number 15 with the key 111000

Key=111000

15 = 001111

110111 = μ

**2.** Now, how can we decrypt encrypted text? Break the text into six digits and restore original letters using XOR.

Here is an encrypted text with private key 111111

111000110000110000111011111111111011111110100110

Go ahead, decrypt in your Notes. Let's see who can be the first one to post the answer here

111111

111000

= 000111 = G

111111

110000

=001111 = O

111111

110000

= 001111 = O

111111

111011

= 000100 = D

111111

111111

= 000000 = space

111111

111011

= 000100 = D

111111

111110

= 000001 = A

111111

100110

= 011001 = Y

**3.** who can tell me why 7^x mod 11 is ONE\_WAY function?

7^x mod 11 is a one-way function. It is hard to reverse.

4.  Alice's private key is 5 and Bob's private key is 3:

**Step 1**.

* Alice chooses a number, say 5, and keeps it secret. We label her number A
* Bob chooses a number, say 3, and keep it secret. We label his number B

**Step 2**.

* Alice puts 3 into the one-way function and works out the result of 75 mod 11= 10. Let us call the result of this calculation α.
* Bob puts 6 into the one-way function and works out the result of 73 mod 11 = 2. Let us call the result of this calculation β.

**Step 3**.

* Alice sends α to Bob.
* Bob sends β to Alice.

**Step 4**.

* Alice computes k = βA mod 11 = 25 mod 11=10
* Bob computes k’ = αB mod 11 = 103 mod 11=10

Obviously, k=k’

5.

Xor the same thing twice with the key gives the same number.

l **= 001100**

10 XOR 001010

001100

001010

000110 - sent to alice

she will again XOR with 10 and get the same initial value

000110

xor  001010

 =  **001100 = l**