

## Tutorial 4 Question 3 (Page 159 in Textbook)

### **What we have :**

$p$  is a large prime

Message  $m$  from Alice to Bob

$$1 \leq m \leq p-1$$

Alice chooses  $a$ , where  $\gcd(a, p-1) = 1$

Bob chooses  $b$ , where  $\gcd(b, p-1) = 1$

To send the message from Alice to Bob, Alice sends

$$c = m^a \pmod{p}$$

to Bob.

Bob sends

$$d = c^b \pmod{p}$$

back to Alice

Alice knows  $a$  and thus can easily compute the inverse of  $a \pmod{p-1}$ . Let the inverse be  $a^{-1}$ .

Alice thus sends

$$e = d^{a^{-1}} \pmod{p}$$

and sends  $e$  to Bob.

To get the message  $m$ , Bob calculates the inverse of  $b \pmod{p-1}$ . Let the inverse be  $b^{-1}$ . He can then retrieve the message by raising  $e$  to  $b^{-1}$ , ie.

$$m = e^{b^{-1}} \pmod{p}$$

To see why it works, recall

$$\begin{aligned} e &= d^{a^{-1}} \pmod{p} \\ &= (c^b)^{a^{-1}} \pmod{p} \\ &= ((m^a)^b)^{a^{-1}} \pmod{p} \end{aligned}$$

$$= (m^{a^l})^b \pmod{p}$$

but  $aa^l = 1 \pmod{p-1}$

so we get

$$e = m^b \pmod{p}$$

By calculating

$$e^{bl} \pmod{p} = m^{bb^l} \pmod{p}$$

and since  $bb^l = 1 \pmod{p-1}$

we get

$$m \pmod{p}$$

### **Example**

Suppose  $p = 101$   
 $p-1 = 100$   
 $a = 3$   
 $b = 7$   
 $m = 15$

Using Extended Euclidean Algorithm,  
we determine that

$$a^l = 67$$

$$b^l = 43$$

$$c = 15^3 \pmod{101} = 42$$

$$d = 42^7 \pmod{101} = 93$$

$$e = 93^{67} \pmod{101} = 99$$

Taking

$99^{43} \pmod{101} = 15$ , we get back the original message.