Assignment 2

**Number Theory**

**(a). Answer the following: (i) What is the size of group Z\*11? (ii) Is 3 a generator of Z\*11? and (iii) Is 2 a generator of Z\*11?**

i)

Z\*11 = { 1,2,3,4,5,6,7,8,9,10}

ii) No because 30 mod 11 = 1 and 35 mod 11 = 1

iii) YES

20 mod 11 = 1

21 mod 11 = 2

22 mod 11 = 4

23 mod 11 = 8

24 mod 11 = 5

25 mod 11 = 10

26 mod 11 = 9

27 mod 11 = 7

28 mod 11 = 3

29 mod 11 = 6

**Key Exchange**

**(a). Suppose p be a prime number and g be the generator of Z ∗ p . Consider a scenario where two users Alice and Bob want to generate a shared key secretly on an open channel using the Diffie-Hellman Key-Exchange Protocol. Let us assume that p = 11, g = 2 and say Alice and Bob choose 3 and 8, respectively, as their random input integers in the Diffie-Hellman Protocol. What would be the final key shared by Alice and Bob under this case? Please explain your answer**

p = 11

g = 2

a = 3

b = 8

Alice sends ga mod 11 => 23 mod 11 = 8

Bob send gb mod 11 => 28 mod 11 = 3

Then

Alice computes 3a mod 11 => 33 mod 11 = 5

Bob computes 8b mod 11 => 88 mod 11 = 5

Therefore the final shared key would be 5

**Public-key Encryption**

**(a). Describe why textbook RSA is not CPA-secure. A solution often used to address this issue is called Padded-RSA. Please explain how Padded-RSA addresses the issue of textbook RSA?**

Textbook RSA is not CPA-secure because it is deterministic, meaning that the same plaintext ‘m’ would produce the same ciphertext.

M1 ---🡪 m’ = C’

M2 ---🡪 m’ = C’

Padded-RSA addresses this issue by adding a random number to ‘m’

M1 ---🡪 r+m’ = C’

M2 ---🡪 r+m’ = C’2

Since r is random then every time m is used it a different C’ would be generated