LAB 6

a) Two users Alice and Bob want to agree on a secret key over a public

network. They have agreed to use the Diffie Hellman algorithm to

achieve this. Given the values below what will be the value of the

shared secret key generated by Alice and Bob?

A random prime : 11

A generator : 3

Alice’s random secret : 4

Bob’s random secret : 5

Step 1: Alice and Bob public no. prime and generator P = 11, G = 3

Step 2: Alice selected a private key a = 4 and

Bob selected a private key b = 5

Step 3: Alice and Bob compute public values

Alice: x =(G^a mod P) = (3^4 mod 11) = 4

Bob: y = (G^b mod P) = (3^5 mod 11) = 1

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =1 and

Bob receives public key x = 4

Step 6: Alice and Bob compute symmetric keys

Alice: ka = y^a mod p = 1^4 mod 11 = 1

Bob: kb = x^b mod p = 4^5 mod 11 = 1

Step 7: 1 is the shared secret.

b) Bad RSA

Using the files listed below can you decrypt the flag

• Badrsa.py

• output.txt

