Information Security

Assignment One

Maximum Marks: 10 Resource Person: Dr. Sheraz Naseer

Q1: On the basis of your "Roll number Mod 5", select the asymmetric parameters of RSA algorithm from following: (CLO3) Marks: 4

0. P=7 , q =5, e= 11
1. P=11, q = 3, e = 13
2. P= 11, q = 5, e = 3
3. P = 7, q= 11, e = 17
4. P= 13, q = 3, e =7

Using the abovementioned parameters, **perform** the following operations of RSA algorithm and **show relevant calculations**:

1. Calculate n = P.Q
2. Calculate 'd' such that d.e = 1Mod Φ(n)
3. Clearly state the Public and Private key parameters.
4. Encrypt '8' using public key 'e' and decrypt the result using private key ' d' to recover '8'.
5. Encrypt '17' using public key 'e' and decrypt the result using private key ' d' to recover '17'.

Q2: Calculate Φ(n) for following Integers: (CLO1) Marks: 3

44, 83, 75, 210, 60, 111

Q3: Compare Deffie-Hellman Key Agreement (DHKA) with other key sharing Mechanisms. Calculate the shared secret using DHKA where parameters are as follows (CLO4). Marks: 3

0. P=13, g=2, a=5, b=9
1. P= 13, g=6, a= 4, b= 10
2. P= 17, g= 3, a= 11, b=7
3. P=17, g= 6, a= 8, b=10
4. P=17, g= 11, a = 3, b= 5