**Exercise 9**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. In the Shamir Identity-based signature scheme, assume that p=17, q=11 and e=7, what is the master secret key? If the identity of a user is 88, what is his private key? Suppose that the user chooses r=3, what is the signature of the user on a message 11, where H(37,11)=23? How do you verify the signature?

2. In ElGamal encryption scheme, assume that a prime modulus p = 457 and a generator g=288. If the private key is 23, what is the public key? Encrypt a message m=31 with a random value k=41 and decrypt the ciphertext.

3. In Paillier encryption scheme, assume that p=5, q=7, N=pq=35, g=36, encrypt a message m=3 with a random value r=2.