**Exercise 4**

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

1. What is a public key encryption scheme?

2. What is a digital signature scheme?

3. What are RSA public key parameters?

4. How does a user choose a public key?

5. How does a user determine the private key?

6. Given a message and Alice’s public key parameters, how does Bob encrypt the message?

7. After Alice receives a ciphertext from Bob, how does Alice decrypt the ciphertext?

8. With fast exponentiation algorithm, how many modular multiplications are needed to compute

m181 (mod n)?

9. Why does the RSA security base on big integer factorization?

10. Why does the RSA security base on discrete logarithm?

11. Perform encryption and decryption using RSA algorithm with the following parameters:

p=13, q=17, e=5, M=2.

12. Perform signature generation and verification using RSA algorithm with the following parameters:

p=13, q=17, e=5, M=3.