**Exercise 8**

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

1. Describe the Lamport’s One-Time Password (OTP) protocol.

2. What are online dictionary attack to password-based authentication? How can you prevent this attack?

3. Describe the encrypted key exchange (EKE) protocol and explain how it can prevent offline dictionary attacks.