Name: **Student's ID**:

CLASS PREP 3

Directions. After reading the section 3.4 and 3.5, please answer the following questions (either directly on the template or on separate paper). This class prep assignment will be **graded on effort.** Please do not leave any questions blank – if you are stuck, either formulate a question that you believe will help you get unstuck or write down some preliminary ideas.

1. What are two factors that the security of any encryption scheme depends on?

Two factor that the security of any encryption scheme depends on is the key length and the strength of the algorithm

2. Who invented public key cryptography and when?

Public key cryptography was invented by Whitfiield Diffe and Martin Hellman
from Stanford University in 1976

3. How many keys do we need in public key cryptography? What are they?

In public key cryptography, we needs 2 keys, which is public and private key. This is a pair of key that have been selected so that if one is used for encryption, the other is used for decryption

4. What are application categories of public-key cryptography? In which application, we use our private key to "sign" the message?

Public-key cryptography has three main application categories: encryption/decryption, digital signatures, key exchange / key establishment
We use our private key to "sign" the message in the digital signature application of public-key cryptography.