Title: CSCI 55500 Homework #4 report
Name: Zhihao Cao
Data: 11/9/2016
Instructor: Xukai Zou
Programming language: Java
Development software: Eclipse

2. A protocol using multi-party computation algorithms can achieve this job. To maintain the security during the private information is transmitting, cryptography applies. Assuming the protocol using asymmetric-key system. The public key is public known by ten professors. Each professor uses the public key to encrypt his/her salary, and shares the encrypted result. The protocol uses its private key to decrypt ten professor's encrypted result, and then calculates the average salary. The protocol uses its private key to encrypt the average salary and share the result to ten professors. Each professor uses public key to decrypt the result to obtain the average salary.

3.

```
Question 1:
Q = mP = (8,15)

Question 2:
Decompress:
(18,27)
(3,3)
(17,26)
(28,6)
m*Decompress:
(15,8)
(2,9)
(30,29)
(14,19)
Plaintext:
20
9
12
5

Question 3:
Convert into English word:
tile
```