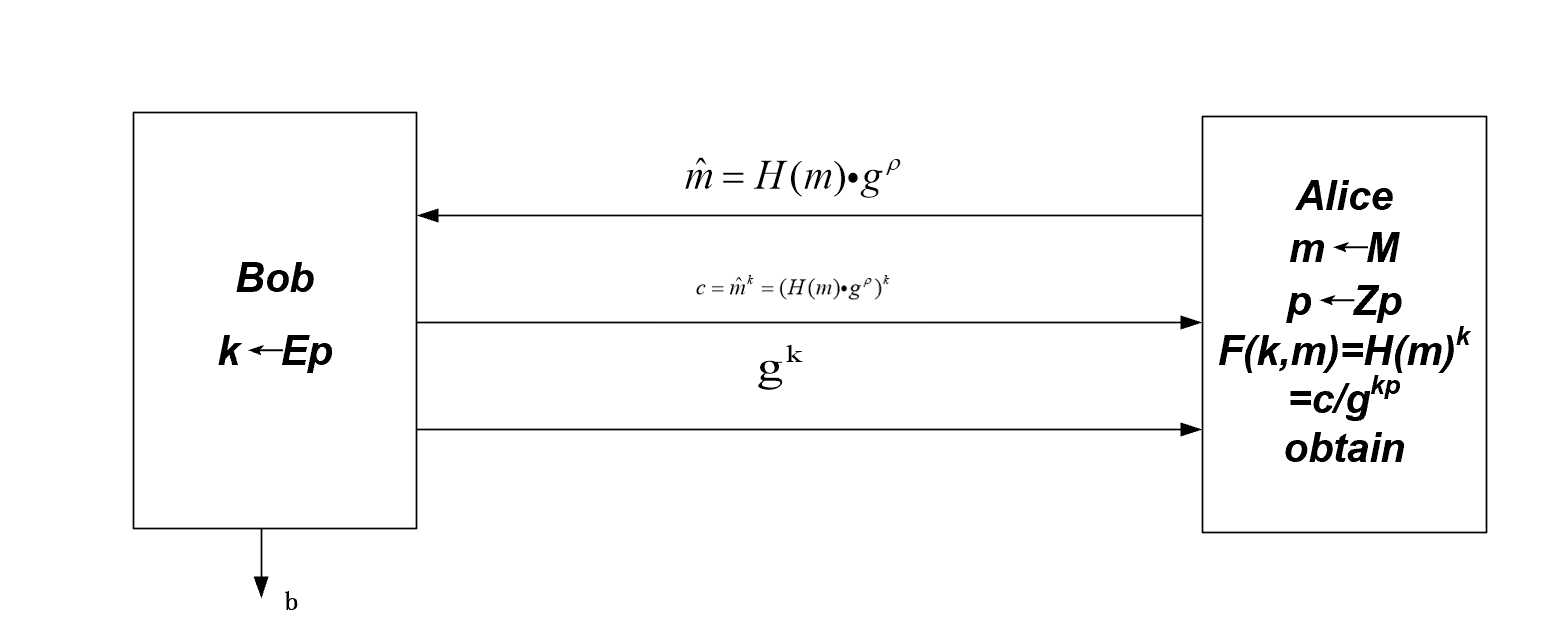
Name: Yitian Shan

Student Number: 202118022

UOW Number: 7377587

Date: 2021/11/20

Question 1



According to the question, we can know Alice will send  to Bob, then Bob can calculate and . and send them to Alice. Therefore, Alice can calculate F(k,m).

Question 2

(1)



When Adversary A outputs : if then output 1, else output 0.

Firstly, I can set B as the game between Challenger (DDH) and Adversary A.

So the  (1)

In addition, we can get  (2)

From the formula (1) and (2), we can get 

So  is semantically secure assuming the DDH assumption holds in G. .

(2) If the DDH assumption does not hold in G,  is non-negligible. Adversary A can distinguish whether is a DH-triple. So A can attempt many different b, then to do encryption and judge if is a DH-triple. if it’s true, the advantage will be equal to 1 and it is not semantic security.

(3) According to the question, we have plaintext *m*1*, m*2, and  ,.If, then 

so it has the property which is called multiplicative homomorphism.

(4)