Name: Yitian Shan

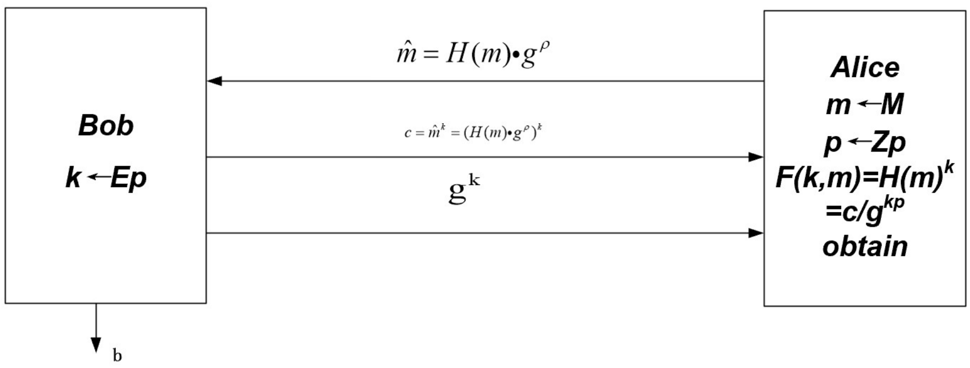
Student Number: 202118022

UOW Number: 7377587

Date: 2021/11/20

---

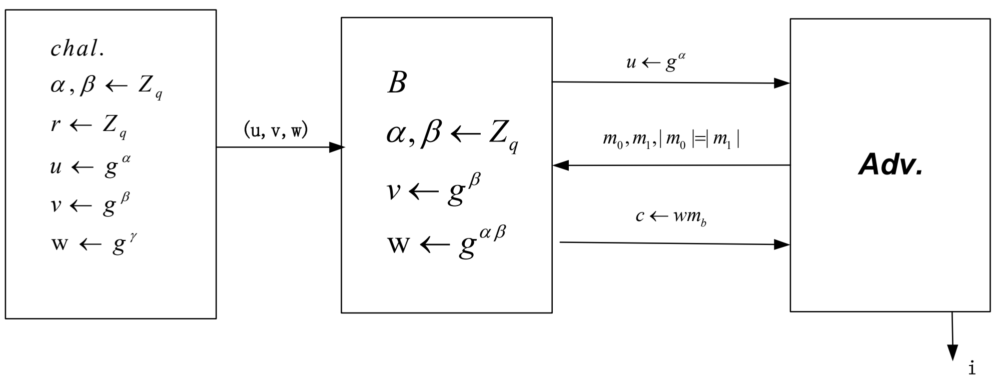
Question 1




According to the question, we can know Alice will send $\hat{m}$ to Bob, then Bob can calculate $c = \hat{m}^k$ and $g^k$. and send them to Alice. Therefore, Alice can calculate F(k,m).

Question 2

(1)




When Adversary A outputs $i'$ : if $b = b'$ then output 1, else output 0.
Firstly, I can set B as the game between Challenger (DDH) and Adversary A.
So the $Adv[A, E_{MEG}] = |\Pr[W_0] - 1/2|$ (1)

In addition, we can get $|\Pr[W_0] - \Pr[w_1]| = Adv_{DDH}[B_{DDH}, G]$ (2)

From the formula (1) and (2), we can get $\Pr[W_1] = 1/2$

So $E_{MEG}$ is semantically secure assuming the DDH assumption holds in G.

$Adv[A, E_{MEG}] = Adv_{DDH}[B_{DDH}, G]$.

(2) If the DDH assumption does not hold in G, $|\Pr[W_0] - \Pr[w_1]| = Adv_{DDH}[B_{DDH}, G]$ is non-negligible. Adversary A can distinguish whether $(u, v, w)$ is a DH-triple. So A can attempt many different b, then to do encryption $\hat{c} = \mathrm{u}^{\mathrm{b}} m$ and judge if $(u, v, \mathrm{u}^{\mathrm{b}})$ 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 $E(pk, m_1) = c_1 = u^{\beta 1} \cdot m_1$, $E(pk, m_2) = c_2 = u^{\beta 2} \cdot m_2$. If $m = m_1 \cdot m_2$, then

$$c = c_1 \cdot c_2 = u^{\beta 1} \cdot m_1 \cdot u^{\beta 2} \cdot m_2 = u^{\beta 1 + \beta 2} \cdot m_1 \cdot m_2 = E(pk, m_1, m_2)$$

so it has the property which is called multiplicative homomorphism.

(4)