

**CSCI971 Advance Computer Security:
Homework #9**

**Mei Wangzhihui
2019124044**

Problem 1

This protocol is like ElGamal encryption mode.

The $sk \leftarrow k, pk \leftarrow g^k$.

Alice knows the public key pk and $F(k, m) = H(m)^k$, she chooses a random $\rho \leftarrow Z_q$ and sends Bob $\hat{m} = H(m) \cdot g^\rho$.

We assume $v \leftarrow g^\rho, \omega \leftarrow pk^\rho = g^{\rho k} = v^k$.

When Bob gets the \hat{m} , he responds $res = \hat{m}^k = H(m)^k \cdot g^{\rho k} = H(m)^k \cdot \omega$ to Alice, as $H(m)$ is a random oracle, so Bob cannot know the m from $H(m)$.

When Alice gets the res , she knows $\omega = g^{k\rho}$ so she just gets $H(m)^k = res/(g^{k\rho})$.

Because it is hard to get k from \hat{m}^k as it is a hard problem in number theory. So Alice doesn't know k .

Problem 2

Game 0

Barcelona Reasonable.

Game 1

sdfas

Problem 3

Problem 4