CSCI971 Advance Computer Security: Homework #9

Mei Wangzhihui
2019124044

Problem 1

This protocol is like EIgamal encryption mode.
The $sk \leftarrow k, pk \leftarrow g^k$.
Alice knows the public key pk and $F(k, m) = H(m)^k$, she choose a random $\rho \leftarrow Z_q$ and sends Bob $\widehat{m} = H(m) \cdot g^\rho$.
We assume $v \leftarrow g^\rho, \omega \leftarrow pk^\rho = g^{\rho k} = v^k$.
When Bob get the $\widehat{m}$, he respond $res = \widehat{m}^k = H(m)^k \cdot g^{\rho k} = H(m)^k \cdot \omega$ to Alice, as $H(m)$ is random oracle, so Bob cannot know the m from $H(m)$.
Wh en Alice get the res, she knows $\omega = g^{k\rho}$ so she just get $H(m)^k = res/(g^{k\rho})$.
Because It is hard to get k from $\widehat{m}^k$ as it is a hard problem in number theory. So Alice doesn't know k.

Problem 2

Alice and Bob there are anything

Problem 3

Problem 4