作业一 HMQV 协议分析

1.Diffie-Hellman 协议是否存在协议漏洞？为什么

2.HMQV 协议是如何弥补 DH 协议中的漏洞的？

3.HMQV 协议中有两个参数 d=H(X,”Bob”)和 e=H(Y,”Alice”)，这两个参数是将发送值与意定的通信方身份进行绑定哈希。这样的处理方式是否冗余？改为 d=H(X)和 e=H(Y)是否有什么安全缺陷？（给出思路即可得分，如果能给出实际的攻击方案可以酌情加分）