一、1. 简述MAC能否解决消息发送方和接收方冲突时的消息不可否认性，为什么?

2. 简述对公钥密码系统攻击中的穷举攻击.

二.1. RSA $p=3$ $q=11$ $d=7$ $M=4$ ~~求M~~，求C并解密

2. ElGamal $p=19$ $\alpha=3$ $X_A=2$ $X_B=5$ $m=7$ m从A到B. $k=5$

计算(C_1,C_2)并解密.

(3) 中国剩余定理. $x\equiv 4 \pmod 5$ $x\equiv 2 \pmod 7$ $x\equiv 5 \pmod{11}$

三.(1) ~~简述~~ 描述CFB，以及为何CFB不容易受报文流篡改，而容易受ee错误传播

(2) ID(Alice)和ID(Bob)表示身份信息，Cert(Alice)，Cert(Bob)表示公钥证书.

$Sig_{Alice}()$，$Sig_{Bob}()$表示私钥签名，如何攻击以下协议.

Bob　　　　　　　　　　Alice.

random r_1 —— Cert(Bob), r_1 ——→

random r_2

计算 $y_1 = Sig_{Alice}(ID(Bob)\|r_1\|r_2)$.

~~random r_2~~

←—— y_1, r_2, cert(Alice) ——

使用Cert(Alice)

验证Alice公钥Ver(Alice)

~~Ver(Alice~~

$Ver_{Alice}(ID(Bob)\|r_1\|r_2, y_1)=true$

成立则接受，否则拒绝.

random r_3

计算 $y_2 = Sig_{Bob}(ID(Alice)\|r_2\|r_3)$

—— y_2, r_3 ——→

计算 $Ver_{Bob}(ID(Alice)\|r_2\|r_3, y_2)=true$.

四. 1. hash函数的性质

2. 数字签名的目的.

3. X.509不包含下列哪些信息.

4. Kerberos认证协议中，AS和TGS共享____

5. ~~欧拉~~ $\varphi(85)=$____