

1. 简述 MAC 能否解决消息发送方和接收方冲突的问题，不可靠性，为什么？
2. 简述密码学在网络安全中的重要性。

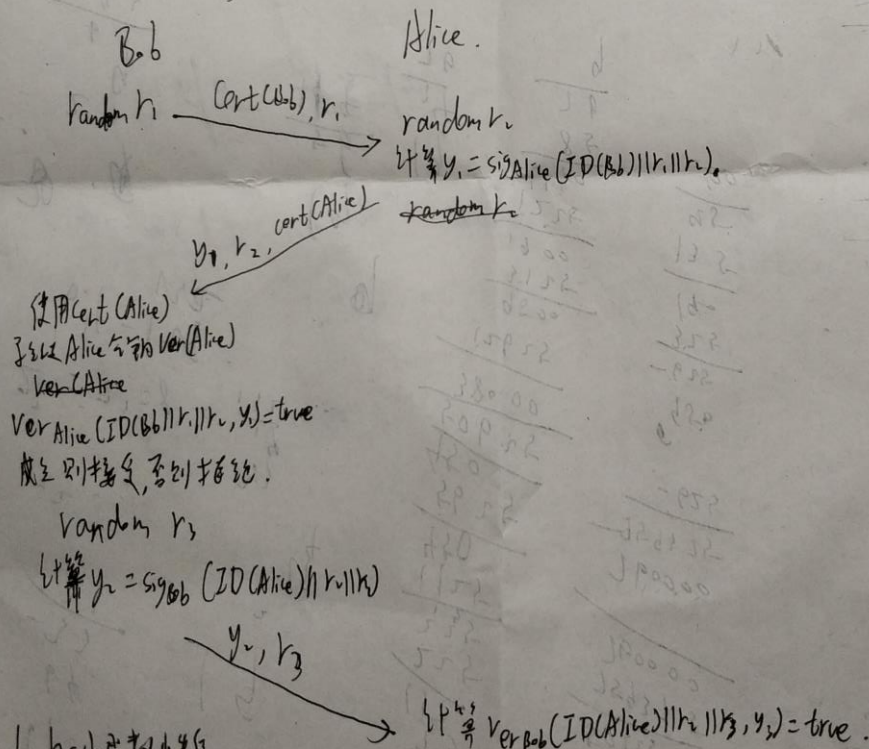
二. 1. RSA  $p=3, q=11, d=7, M=4$  并解密

2. ElGamal  $p=19, \alpha=3, X_A=2, X_B=5, m=7$  在 A 到 B.  $lc=5$   
计算  $(1,1)$  并解密.

(b) 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 CFB, 以及为何 CFB 不需要对明文流篡改, 而需要对密文流篡改.

(2)  $ID(Alice)$  和  $ID(Bob)$  表示身份标识,  $Cert(Alice), Cert(Bob)$  表示公钥证书.  
 $Sig_{Alice}()$ ,  $Sig_{Bob}()$  表示签名. 如何防止以下攻击.



四. 1. hash 函数性质

2. 数据完整性验证

3. X.509 不包含下列哪条信息.

4. Kerberos 认证协议中, AS 与 TGS 共享

$$5. \phi(85) = \underline{\hspace{2cm}}$$