1. p,q为素数，n=pq=3599，Φ（n）=3480, 求出p和q是多少?

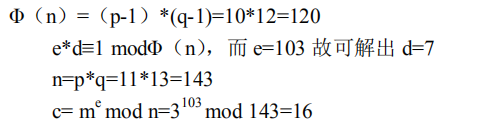
解：Φ（n）=（p-1）（q-1）=3480

n=pq=3599

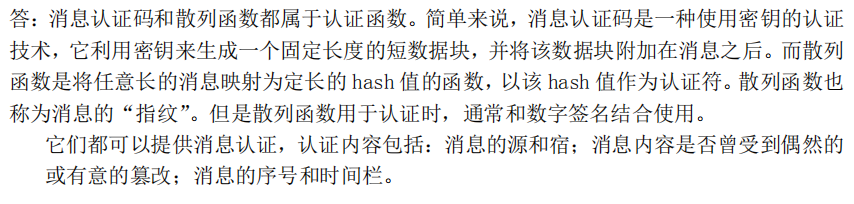
p=59 ，q=61

1. 利用 RSA 算法运算，如果 p=11，q=13, e=103,对明文 3 进行加密,求密文?用户的私钥d等于多少?

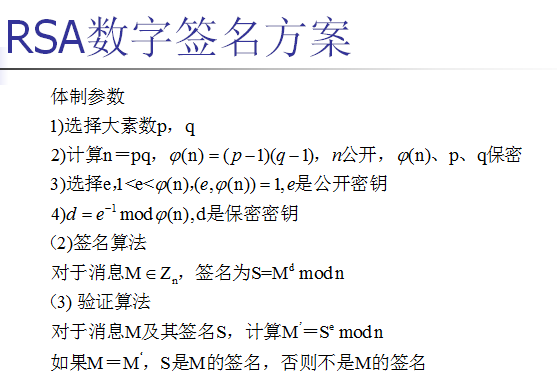
解：

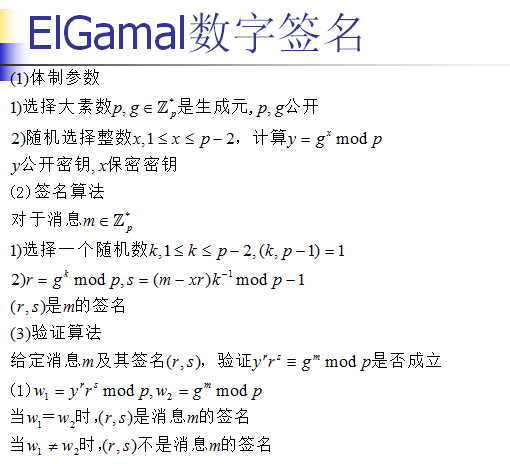


1. 散列函数和消息认证码有什么区别？各自可以提供什么功能？



1. 描述RSA和ElGamal数字签名方案。





1. 在ElGamal数字签名方案中，如果签名时的随机数k泄露了，对数字签名方案有什么安全影响。

