

2.用模算术描述Caesar加密算法.

3.为什么加密算法应该公开？

4.一次一密(OTP)是无条件安全的，但它为什么不实用？





1、如果明文和密钥全是1，DES算法的第一轮输出是什么？（16进制表示）

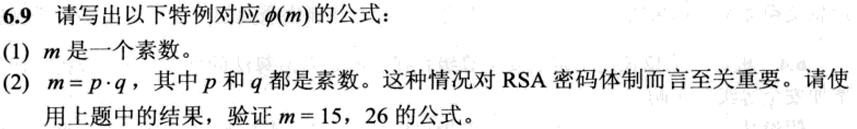
如果明文和密钥的所有位（bit）都为1，经过DES算法的第一轮加密后，其64位的输出结果为 **FFFFFFFFFBEE5665**

2、分组加密算法DES明文长度只有64位，如果你想加密一个长文档。回答如下问题。

2.1、为什么推荐使用 分组链接模式（CBC）模式，而不是直接使用 电子密码本（ECB）模式？（列举主要原因）

2.2、如果使用 ECB 加密图片，会发生什么？

如果使用ECB模式加密一张图片，加密后的图片虽然像素颜色会变得混乱，但原始图片的轮廓和结构依然会清晰可见。



2、公钥密码学与对称密码学的核心区别是什么？——从密钥数量与工作原理两个角度分析

3、公钥密码学相比对称密码学的主要优势是什么？

4、公钥密码学的出现是否导致对称密码学被淘汰？为什么？

5、在处理大规模数据加密时，人们通常采用混合加密。请简述其工作原理。

1、辗转相除法计算gcd(7469,2464)，写出步骤

2、求模7运算下3的逆元，即3^（-1）mod 7

3、假设p=41,q=17,公钥e1=32, e2=49，哪个是合法的公钥，请解释合法公钥所需要满足的条件

4、假设p=3,q=11,e=3, 回答如下问题。

4.1当明文x=5时，计算密文

4.2当密文c=10时，计算明文

1、请使用扩展欧几里得算法计算以下数值的最大公约数和参数x,y （写出步骤）

(1) 198 和 243

(2) 1819 和 3587

2、请使用平方-乘算法下面的指数运算 x^e mod n（写出步骤）

(1) x=2,e=79,n=101

(2) x=3,e=197,n=101

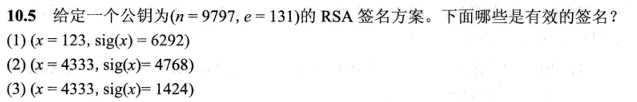
3、RSA 加密算法中，当Alice选择明文m,使得gcd(m,n)=1时， 加密c=m^e mod n。 请问为什么Bob解密c^d mod n能得到m? （写出推导步骤）

4、今天是星期一，2^2400天后是星期几？（应用费马小定理计算）

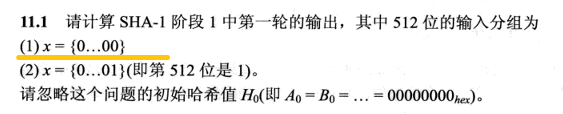
1、公钥加密和数字签名是基于公钥密码体制的两种重要应用，但在设计目标和使用方式上存在显著差异。

1.1从安全目标和密钥使用方式两方面，简述数字签名和公钥加密的区别?

1.2在软件发布过程中，开发者通常对软件包生成数字签名，并公开发布签名和公钥。请分析这样做能防止哪些类型的攻击？



1、哈希函数的3个安全性定义。



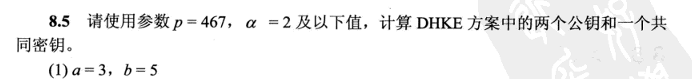
3、数字签名和消息认证码主要区别？

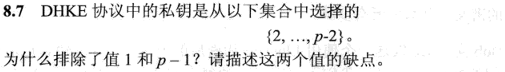
4、学生从大学官方网站下载考试成绩单的场景中，为了确保文件未被篡改且确实由学校发布，应使用数字签名还是消息认证码？请简要说明理由。

5、在一家公司内部，财务系统定期将加密后的工资表发送给人力资源系统处理。在此过程中，为了验证数据的完整性和确实来源于财务系统，应使用数字签名还是消息认证码？请简要说明理由。

6、一名艺术家准备对自己创作的高清图片进行数字签名。请解释为什么他通常会先对图片进行哈希运算，再对哈希值进行签名？这样做能提高效率吗？为什么？

7、在一个在线游戏的下载过程中，用户设备被恶意软件感染，导致下载的游戏安装包被篡改。游戏开发者在官方网站上同时提供了安装包的哈希值。请问用户应如何利用这个哈希值检测安装包是否被篡改？





1、数字证书是谁颁发的？

2、数字证书的基本格式是什么？

3、A想和B通信，当A接收到B的证书C(B)时，敌手O把它替换成自己的合法证书C(O)，A如何检测这么伪造？

4、接上题，当A接收到B的证书C(B)时，如敌手O只是将C(B)中公钥替换成自己的公钥，A如何检测这么伪造？