作业 2

PB19111708 杨云皓

1. 一个密码系统包括哪些要素？

明文空间、密文空间、密钥空间、加密算法和解密算法

2. RSA 算法的理论基础是什么？简述 RSA 算法的流程。

理论基础是数论中“大整数的素因子分解是困难问题”的结论，即求两个大素数的乘积在计算机上时是容易实现的，但要将一个大整数分解成两个大素数之积则是困难的。

流程：

（1）密钥计算方法：

① 选择两个大素数 p 和 q（典型值为 1024 位）

② 计算 n=p q 和 z=(p-1) (q-1)

③ 选择一个与 z 互质的数，令其为 d

④ 找到一个 e 使满足 e d =1 (mod z)

⑤ 公开密钥为 (e, n)，私有密钥为 (d, n)

（2）加密方法：

① 将明文看成比特串，将明文划分成 k 位的块 P 即可，这里 k 是满足2^k<n 的最大整数。

② 对每个数据块 P，计算 C＝P^e (mod n)，C 即为 P 的密文。

（3）解密方法：

对每个密文块 C，计算 P＝C^d(mod n),P 即为明文。

(4)密钥计算：

① 取 p＝5，q＝13

② 则有 n＝p×q=65，z＝(p-1)×(q-1)=(5-1)×(13-1)=48

③ 11 和 48 没有公因子，可取 d＝11

④ 求满足 11×e＝1(mod z)=1(mod 48)的 e，得到 e＝35

⑤ 公钥为(e,n)=(35, 65)，私钥为(d,n)=(11, 65)

(5)加密：

若明文 P＝63，则密文 C＝P^e(mod 65)＝63^{35}(mod 65)＝32。

(6)解密：

计算 P＝C^d(mod n)＝32^{11}(mod 65)＝63，恢复出原文

3. 数字签名和消息鉴别的主要区别是什么？

消息鉴别也称为“报文鉴别”或“消息认证” ，是一个对收到的消息进行完整性和真实性验证的过程。数字签名是手写签名的数字化形式，是公钥密码学发展过程中最重要的概念之一，也是现代密码学的一个最重要的组成部分之一。

4. 假设计算能力遵循摩尔定律，分析三重 DES 目前在计算上是否安全的。

2000 年 1 月，在“第三届 DES 挑战赛”上，EFF 研制的 DES 解密机以 22.5 小时的战绩，成功地破解了 DES 加密算法。今天 2022 年 3 月，与上述时间相差 266 个月，即 15 次摩尔定律生效次数，即当今的计算能力是当时的2^{15}倍。破解 DES3 密文需要2^{112}次穷举搜索，而破解 DES2 则需2^{56}次穷举搜索，即时间复杂度 T（DES3）=2^{56}T（DES2）；所以现在破解时间应为 t=$\frac{2^{56}}{2^{15}} \times 22.5 = 2^{41} \times 22.5$h，所以理论上来说目前 DES3 是安全的。