2020年现代密码学课程设计任务书

同济大学，杨礼珍

2020 年 6 月 22 日

目录

1.基本要求

1.提交方式：发到我的email: yanglizhen_exe@163.com。邮件标题为“学号+姓名+现代密码学课程设计”。

2.提交截至时间：2020年7月10日

3.需提交文档（请以邮件附件的方式发送，附件标题为“学号+姓名+现代密码学课程设计”。不要保存在其他网站中再把链接发给我。如果文档太大请去掉调试过程的中间文件。）：

1. C/C++程序源代码
   - 代码有良好的可读性。切忌一些极差的编程习惯，如只有一个main函数，或全部为全局变量。
   - 程序使用友好。如果是控制台程序，如有大量输入，最好用文件的方式的输入。
2. 可执行文件
3. pdf格式的课程设计说明书

2.编程任务

Alice生成RSA密钥：

1. Alice生成一对RSA公钥(n, b)和私钥(p, q, a)，其中随机素数p, q都为512比特长；或都为1024比特长度；两种长度都需支持。

   要求 基于开源代码NTL实现，NTL为密码界流行的高精度代数数论库。不支持其他方式。NTL网址：https://www.shoup.net/ntl/。网站上或下载下来的文档中有详细的使用说明书。

   注意 为了保证通过素性检测的数是素数的概率足够大，需测试足够的次数，如产生512比特的素数，通过测试的数不是素数的概率（即错误概率）接近$1/2^{512}$。

2. Alice把公钥传给Bob。不需要实现网络传输，下同。

2.编程任务

Bob加密文件m并发给Alice：

1. 输入文件m，m为任意长。如何把文件转成所需要的格式，请自行决定。CBC模式中，如果m的长度不是分组的倍数时，需要填充，如何填充请自行决定，但解密时需要把填充去掉。
2. 生成128比特的随机数k作为临时的会话密钥。
3. 用Alice的公钥加密k得到$c_1 \leftarrow k^b \bmod n$。
4. 用会话密钥k加密文件m得到c_2，其中加密算法为AES，使用CBC模式。

   要求 AES的列混合运算及其逆运算使用我的课件中提供的快速算法。S-Box使用查表方式实现。AES的测试数据可参考AES的flash动画。
5. 把(c_1, c_2)发给Alice。

2.编程任务

Alice解密恢复文件m:

1. 用Alice的RSA私钥解密c_1得到k。
2. 用k解密c_2得到m。
3. 输出m。

2.编程任务

上面所涉及到的随机数（包括随机素数生成，CBC中的IV）请使用ANSI X9.17算法生成，不可使用系统提供的伪随机数函数生成。用于密码用途的随机数需使用专用于密码用途的伪随机数算法生成。

算法ANSI X9.17 伪随机数比特生成器

输入：随机（秘密的）64比特种子s，整数m，两个DES密钥k_1, k_2。

输出：m个64位伪随机比特串$x_1, x_2, \ldots, x_m$。

1. 计算中间值$I = DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(D)))$，其中$D$表示当前日期/时间的精确表示，DES表示DES加密，DES^{-1}表示DES解密。
2. For $i = 1$ to m:
    1. $x_i \leftarrow DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(I \oplus s)))$
    2. $s \leftarrow DES_{k_1}(DES_{k_2}^{-1}(DES_{k_1}(x_i \oplus I)))$
3. 返回$x_1, x_2, \ldots, x_m$。

2.编程任务

注意：

- 我课件虽然给出了DES的完整描述，但没有仔细核对每个表格。请下载DES的标准文档查找各个表格的准确描述，或《应用密码学手册》第7章http://cacr.uwaterloo.ca/hac/about/chap7.pdf。
- 除去奇偶校验位后，DES密钥的实际长度为56位。
- DES测试向量：明文“Now is the time for all ”，表示为8比特的十六进制数（7比特ASCII码，加上0比特的前缀），DES密钥的十六进制表示为K = 0123456789ABCDEF，得到下面的明文/密文对:

  P = 4E6F772069732074 68652074696D6520 666F7220616C6C20

  C = 3FA40E8A984D4815 6A271787AB8883F9 893D51EC4B563B53

3.课程设计说明书要求

- 需包含本人学号、姓名、标题。
- 包含程序设计说明。
- 包含程序使用说明，包括输入格式，输出格式等，并给出具体例子的详细截图。