实验一、古典密码

**一、实验目的**

通过实现简单的古典密码算法，理解密码学的相关概念如明文（plaintext）、密文（ciphertext）、加密密钥（encryption key）、解密密钥（decryption key）、加密算法(encryption algorithm)、解密算法（decryption algorithm）等。

**二、实验内容**

**1）**用C\C++语言实现**单表仿射**（Affine）加/解密算法；

**2）**用C\C++语言实现统计26个英文字母出现频率的程序；

**3）**利用**单表仿射**加/解密程序对一段较长的英文文章进行加密，再对明文和密文中字母出现的频率进行统计并作对比，观察有什么规律。

仿射变换：

**加密**：

**解密**：

其中，*k*1和*k*2为密钥，*k*1∈*Zq*，*k*2∈*Zq*\*。

**实验要求：**加/解密程序对任意满足条件的*k*1和*k*2都能够处理。

实验二、序列密码

**一、实验目的**

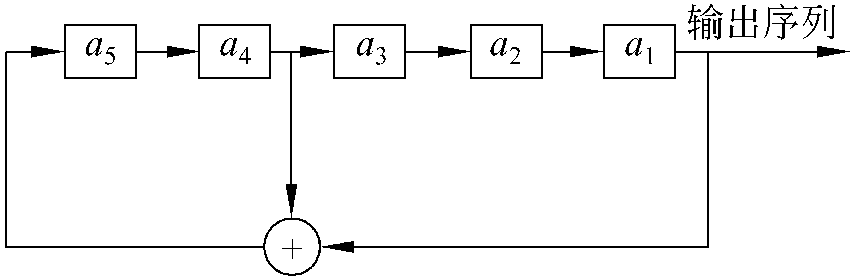
通过实现简单的线性反馈移位寄存器（LFSR），理解LFSR的工作原理、本原多项式的重要意义。

**二、实验内容**

**1）**利用C\C++语言实现给定的LFSR；

**2）**通过不同初始状态生成相应的序列，并观察它们的周期有什么特点；

**3）**利用生成的序列对文本进行加/解密（按对应位作模2加运算）。

给定的LFSR为：

实验三、DES算法的实现/AES算法的实现

（二选一）

**一、实验目的**

通过实现DES/AES算法，加深对DES/AES算法的理解，同时学习组合密码常用的代换、移位等运算的实现。

**二、实验内容**

**1）**利用C\C++实现DES/AES算法的加、解密运算。

实验四、RSA算法的实现

**一、实验目的**

掌握并实现RSA算法。

**二、实验内容**

利用C\C++实现RSA算法的加、解密运算。

具体包括：

1. 利用扩展的Euclid计算 *a* mod *n* 的乘法逆元；
2. Miller-Rabin素性测试算法对一个给定的大数进行测试；
3. 实现的运算，并计算；
4. 利用Euler定理手工计算，并与**3）**计算的结果对比；
5. 实现RSA算法。并对"I LOVE NANJING UNIVERSITY OF AERONAUTICS AND ASTRONAUTICS"加解密。说明：为了方便实现，分组可以小一点，比如两个字母一组。

|  |  |
| --- | --- |
| 字母及其数字编码 | 字母及其数字编码 |
| 空格 00 | N 14 |
| A 01 | O 15 |
| B 02 | P 16 |
| C 03 | Q 17 |
| D 04 | R 18 |
| E 05 | S 19 |
| F 06 | T 20 |
| G 07 | U 21 |
| H 08 | V 22 |
| I 09 | W 23 |
| J 10 | X 24 |
| K 11 | Y 25 |
| L 12 | Z 26 |
| M 13 |  |

实验五、数字签名算法

**一、实验目的**

通过实现数字签名算法（DSA），加深对数字签名算法的理解，同时学习Hash算法的实现。

**二、实验内容**

**1）**利用C\C++语言实现DSA算法。

**2）**DSA中的Hash函数采用SHA算法。