

密码学课程设计说明文档

学号 102381

姓名 何金海

软件设计说明书

程序完成课程设计所有必做与选做的要求，包含的函数如下：

BlockType SBox_Encode(BlockType x) S 盒置换

BlockType SBox_Decode(BlockType x) S 盒逆变换

BlockType PBox_Encode(BlockType x) P 盒置换

BlockType PBox_Decode(BlockType x) P 盒逆变换

void OutPut_Bin(BlockType p)输出显示一个 16 位二进制数

void OutPut_Key(KeyType key)输出显示一个密钥

void BlockEncryption(BlockType PlainText,BlockType
&CipherText,KeyType Key)

分组加密函数

void BlockDecryption(BlockType &PlainText,BlockType
CipherText,KeyType Key)

分组解密函数

void Key_Engine()生成指定密钥

void Key_Random()随机生成密钥

int FileEncryption(char *PlainFile,char *CipherFile,KeyType Key)

文件加密

int FileDecryption(char *PlainFile,char *CipherFile,KeyType Key)

文件解密

unsigned long EncryptionTime(unsigned long Times)

加密函数的运行速度

BlockType LinearCryptanalysis(unsigned long T,BlockType Text[][2])

线性密码分析

BlockType DiffCryptanalysis(unsigned long T,BlockType Text[][4])

差分密码分析

void TestBlockEncrypt()测试分组加密与解密

void TestFileEncrypt()测试文件加密与解密

void TestEncryptionTime()测试运行速度

void TestLinearCryptanalysis()测试线性密码分析

void TestDiffCryptanalysis()测试差分密码分析

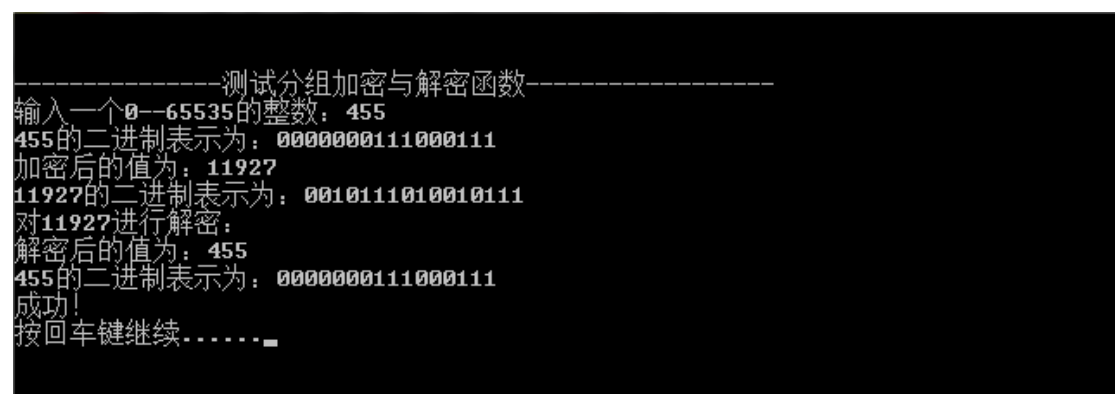
void TestLinearSucceedTimes()测试线性分析函数成功时明密文对数

void TestDiffSucceedTimes()测试差分分析函数成功时明密文对数

void Wait()暂停，按回车键继续

测试程序只需打开生成的可执行文件，按提示操作即可。

运行截图如下：



```
-----测试分组加密与解密函数-----
输入一个0--65535的整数: 455
455的二进制表示为: 0000000111000111
加密后的值为: 11927
11927的二进制表示为: 0010111010010111
对11927进行解密:
解密后的值为: 455
455的二进制表示为: 0000000111000111
成功!
按回车键继续.....
```

任意输入一个小于 65536 的非负整数，即可进行 16 位数据分组加密与解密的演示。

```

-----测试文件加密与解密函数-----
输入文件名: d:\CWork\in.txt
加密后的文件名为: d:\CWork\in.txt.cip, 请手动查看。
按回车键继续.....
对文件d:\CWork\in.txt.cip进行解密:
已解密, 文件名为d:\CWork\in.txt, 请手动查看
按回车键继续.....

```

测试文件加密与解密：请确保输入的“目录\文件名”正确，否则会返回“文件不存在，失败”。对文件加密之后会在原目录中生成加密文件“文件名.cip”，继续则会自动进行解密，重新在原目录下生成新的原文件，建议文件加密之后将原文件移至其他地方，再进行解密操作，方能见到文件解密效果。

文件加密对任意文件格式有效。

接下去的步骤是测试平均加密时间，采用 1000 个随机密钥分别对 0—65535 的每个数进行加密，给出平均一个密钥所用的加密时间。

```

-----测试平均加密时间-----
此过程大约需要2分钟，请耐心等待.....
共对0--65535的值加密1000次，平均加密时间为 81毫秒。

```

下面会测试线性密码分析与差分密码分析，随机产生的明密文对分别为 8000 与 100 对。此过程可能成功或失败，猜想失败可能与随机明文的产生有关。

```

-----测试线性密码分析-----
所分析的密钥为 0000011000001010
分析得出的密钥为0000011000001010
成功!
按回车键继续.....

-----测试差分密码分析-----
所分析的密钥为 0000100100000011
分析得出的密钥为000000000000011
失败! 可能与随机明密文对的产生有关

```

最后进行密码分析成功时的明密文对数量的测试。

附带程序：

随作业附带的可执行文件 `FileEncryption.exe` 可方便地进行文件的加密与解密。示例如下：

```
***** 1 -- 加密文件 *****
***** 2 -- 解密文件 *****
***** 0 -- 退出 *****
请选择0--2: 2
请按顺序输入加密所用的五个正整数密钥，以空格隔开，输入其他则使用默认密钥: 0 0 0
0 0
请输入要解密的文件的文件名，请确保文件在当前目录下:
test.txt.cip
文件解密成功，解密后文件为test.txt
请选择0--2: 1
请按顺序输入加密所用的五个正整数密钥，以空格隔开，输入其他则使用默认密钥: s
请输入要加密的文件的文件名，请确保文件在当前目录下:
test.txt
文件加密成功，加密后文件为test.txt.cip
请选择0--2: 2
请按顺序输入加密所用的五个正整数密钥，以空格隔开，输入其他则使用默认密钥: test
请输入要解密的文件的文件名，请确保文件在当前目录下:
test.txt.cip
文件解密成功，解密后文件为test.txt
请选择0--2:
```

如图，可自行输入加密所取密钥，也可使用默认密钥。只要对文件解密时所用密钥与文件加密时相同，即可还原原文件，若解密时采用密钥与加密时不同，则可能生成另一个乱码文件或产生错误。

效率

为了提高加密与解密的效率，S 盒与 P 盒以及它们的逆变换直接采用数组存储，使用时采用查表的方式直接查询获得。

移位运算中，尽量将一个数对同一个方向的移位按照从近到远的方式进行，减少重复平移的位数。

测试平均加密时间

```
-----测试平均加密时间-----  
此过程大约需要25分钟，请耐心等待.....  
共对65535的值加密10000次，平均加密时间为 80毫秒。
```

如上图所示，总共对 10000 个随机密钥进行了测试，得到的平均加密时间为 80ms。

测试平台如下：

软件平台：操作系统 WIN7 32 位，编译器 VC6.0

硬件平台：处理器 Intel(R) Core(TM)2 Duo CPU T6570 2.1GHz

内存 4GB

密码分析成功时的明密文对数量

采用 6000—20000 对随机明密文分别进行线性密码分析，明密文对数量每增加 200 测试一次并输出结果“成功”或“失败”。

结果如下：

```
-----测试线性分析函数成功时明密文对数-----  
6000成功  
6200成功  
6400失败  
6600失败  
6800失败  
7000失败  
7200成功  
7400成功  
7600成功  
7800成功  
8000成功  
8200成功  
8400成功  
8600失败  
8800成功  
9000成功  
9200失败  
9400成功  
9600成功  
9800失败
```

10000 成功
10200 成功
10400 成功
10600 成功
10800 成功
11000 成功
11200 成功
11400 成功
11600 成功
11800 成功
12000 成功
12200 成功
12400 成功
12600 失败
12800 成功
13000 失败
13200 成功
13400 成功
13600 成功
13800 成功
14000 成功
14200 成功
14400 成功

14600 成功
14800 成功
15000 成功
15200 成功
15400 成功
15600 失败
15800 成功
16000 成功
16200 成功
16400 成功
16600 成功
16800 成功
17000 成功
17200 成功
17400 成功
17600 成功
17800 成功
18000 成功
18200 成功
18400 成功
18600 成功
18800 成功
19000 成功
19200 成功
19400 成功
19600 成功
19800 成功
20000 成功

采用 50—300 对随机选择明密文分别进行差分密码分析，明密文对数量每增加 10 测试一次并输出结果“成功”或“失败”。

结果如下：

```
-----测试差分分析函数成功时明密文对数-----  
50成功  
60成功  
70失败  
80失败  
90失败  
100失败  
110成功  
120失败  
130失败  
140成功  
150成功  
160失败  
170失败  
180成功  
190成功  
200成功  
210成功  
220成功  
230成功  
240成功  
250成功  
260成功  
270成功  
280成功  
290成功  
300成功
```

由结果可发现，对于线性密码分析与差分密码分析，随着明密文对数量的增加，分析成功的概率都会明显增大，但仍然有一定的可能出现攻击失败的情况，这也许与随机明密文对的产生有关，也可能是我在程序编制过程中没有意识到的错误。

在明密文对取到一定大的值时，线性分析为 7200，差分分析为 180，可近似认为密码分析一定会成功，因为出现失败的概率已经很小。