实 验 报 告

课程名称 密码学基础

学　　院 计算机学院

专　　业 保密管理

姓　　名 王君可

学　　号 **17300240009**

开 课 时 间 **2019** 至 **2020** 学年第 二 学期

实验项目名　　称	DES&AES	成绩	

一、实验目的

1. Implementing DES algorithm　实施 DES 解密和解密算法

2. Understanding usage of AES algorithm　理解用 OPENSSL 进行 AES 解密

二、实验内容

1. Create 16 subkeys, each of which is 48-bits long. 创建子密钥

1.1 用 PC-1 表排序实现：64bits->56bits

1.2 移位然后用 PC-2 分别生成子密钥 K1、K2....K16

2. Encode each 64-bit block of data. 加密数据

2.1 将明文用 IP 表排序得到 L0 和 R0，然后基于以下公式：

$L_n = R_{n-1}$;

$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$

2.2 关于 round function:

$R_{n-1} \rightarrow E(R_{n-1}) \rightarrow K_n \oplus E(R_{n-1}) \rightarrow B1B2 \ldots . B8 \rightarrow S1(B1)S2(B2) \ldots S8(B8) \rightarrow L_{n-1} \oplus f = R_n$

3. use AES in OpenSSL 使用 OPENSSL

三、实验步骤

1. 实现如下四个函数：

Permutation_by_table (block. block_len, table)

Generate_round_keys (C0, D0)

Round_function (Ri, Ki)

Encrypt (msg, key, decrypt=false)

2. 解密 DES 密文

3. 解密 AES 密文

四、实验结果及分析

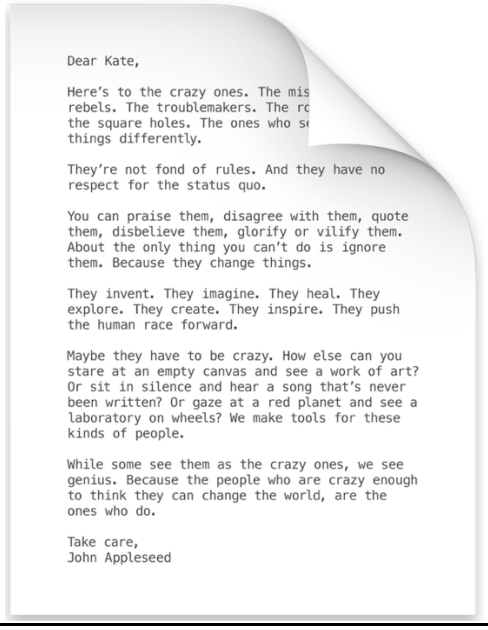
1. plain text: WuhanV5! (for even, the result is ChinaV5!)

```
Plain Text: WuhanV5!
```

2. time for generate keys:0.00036s
   time for run round-function: 5.79e-05s
   time for encrypt/decrypt: 0.0017108s

```
time for key:  0.0003609657287597656
time for f:  8.20159912109375e-05
time for f:  5.984306335449219e-05
time for f:  5.698204040527344e-05
time for f:  5.626678466796875e-05
time for f:  5.602836608886719e-05
time for f:  5.7220458984375e-05
time for f:  5.817413330078125e-05
time for f:  5.626678466796875e-05
time for f:  5.5789947509765625e-05
time for f:  5.698204040527344e-05
time for f:  5.4836273193359375e-05
time for f:  5.793571472167969e-05
time for f:  5.4836273193359375e-05
time for f:  0.00010204315185546875
time for f:  5.793571472167969e-05
time for f:  7.796287536621094e-05
time for encrypt:  0.0017108917236328125
```

3. plain text of AES:



Dear Kate,

Here's to the crazy ones. The mis
rebels. The troublemakers. The rc
the square holes. The ones who s
things differently.

They're not fond of rules. And they have no respect for the status quo.

You can praise them, disagree with them, quote them, disbelieve them, glorify or vilify them. About the only thing you can't do is ignore them. Because they change things.

They invent. They imagine. They heal. They explore. They create. They inspire. They push the human race forward.

Maybe they have to be crazy. How else can you stare at an empty canvas and see a work of art? Or sit in silence and hear a song that's never been written? Or gaze at a red planet and see a laboratory on wheels? We make tools for these kinds of people.

While some see them as the crazy ones, we see genius. Because the people who are crazy enough to think they can change the world, are the ones who do.

Take care,
John Appleseed

五、实验总结

1. 通过实现 DES 算法，深入地了解了 DES 加密算法的加密和解密过程，包括 round function 的实施机制、子密钥的实施机制、加密的过程

2. 其中生成子密钥的时候通过移位生成 C1、D1、C2.....的时候有些移 1 一位有些移两位，我的猜测是正好加起来和的位数是 28 位也就是 C/D 的位数，可以既保证充分利用 28 的长度，又保证不会重复利用子密钥

3. DES 的加密和解密过程的最大区别在于密钥不同，加密使用的是第 i 轮位 Ki, 解密的时候是 K17-i

4. 整个的数据加密过程使用的数据单元主要是 int 类型的整数和 16 进制的字符串、2 进制的字符串，或许都采用 2 进行的字符串可以简化代码提高加密的速度

5. 关于为什么 DES 为什么要使用 16 轮，我的猜测是 C/D 都是 28 位，所以小于 28 但是是 2 的整数次幂的最大数就是 16

6. 通过实现过程发现算法的安全性应该很大程度上依赖于 S 盒、P 盒、E 盒的设计，所以在具体使用的过程种，如果这几个盒是大家通用的话，就是完全依赖于密钥（根据秘密完全寓于密钥是这样，但是这样的话 2^64 感觉用现代计算机破解应该不是不可能）

7. OPENSSL 为我们提供了功能强大、调用方便的加密和解密算法调用接口