# 密码算法实验（一）

**【实验目的】**

 通过对DES算法的代码编写，了解分组密码算法的设计思想和分组密码算法的工作模式。

**【实验仪器】**

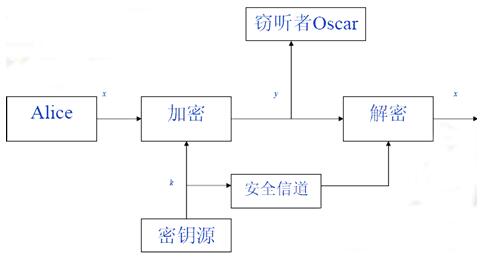
(1)安装Windows操作系统的个人计算机。

(2)安装VC6.0以上版本的编译器。

**【实验原理】**

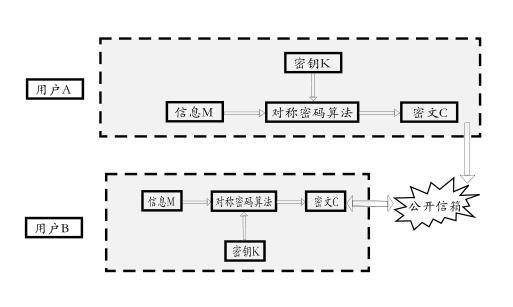
(1) 加密——解密过程

在密码体制中，参与方分为：发信方，收信方及攻击者，有明文，密文，密钥，加密算法，解密算法五大要素。加密和解密过程描述如图10-1所示：



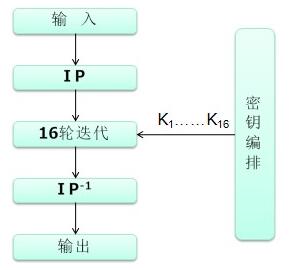
**图10-1** 加密-解密过程原理

对称加解密过程如图10-2所示。

**图10-2** 对称加解密过程

(2) DES算法介绍

DES是Data Encryption Standard（数据加密标准）的缩写。它是由IBM公司研制的一种加密算法，美国国家标准局于1977年公布把它作为非机要部门使用的数据加密标准，二十年来，它一直活跃在国际保密通信的舞台上，扮演了十分重要的角色。DES是一个分组加密算法，分组长度为64b，密钥长度也为64b，但因为含有8个奇偶校验比特，所以实际密钥长度为56b。DES算法是迄今为止使用最为广泛的加密算法，由于计算能力的发展，DES算法的密钥长度已经显得不够安全了，所以目前DES的常见应用方式是DES\_ESE2，即3重DES，采用加密-解密-加密3重操作完成加密，其中加密操作采用同一密钥，有效密钥长度为112b。



**图10-3** DES算法的整体结构

加密过程：

①给定明文，通过一个固定的初始置换IP来重排输入明文块P中的比特，得到比特串P0=IP(P)=L0R0，这里L0和R0分别是P0的前32比特和后32比特。

②按下述规则进行16次迭代，即 1≤i≤16。这里，是对应比特的模2加，f是一个函数（称为轮函数）；16个长度为48比特的子密钥Ki(1≤i≤16)是由密钥k经密钥编排函数计算出来的。

③对比特串R16L16使用逆置换IP-1得到密文C，即C=IP-1 (R16L16) 。

解密过程：

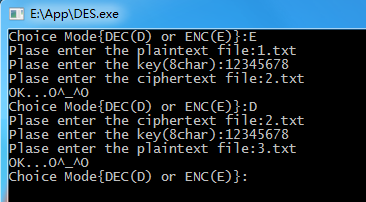
DES的解密与加密一样使用相同的算法，它以密文y作为输入，但以相反的顺序使用密钥编排K16,K15,…,K1, 输出的是明文x。

(2)DES算法源代码

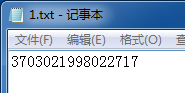
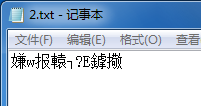
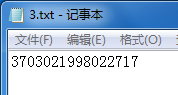
见附件的DES算法CPP源程序。

**【实验内容及步骤】**

自行编写DES算法，利用DES算法程序，以自己身份证前16位为明文，12345678为密钥，得到密文，并解密。如图10-4、10-5所示。



**图10-4** DES算法实现程序

**图10-5** DES算法实现程序结果