

SDES 加密解密程序文档

07300700042 张璞

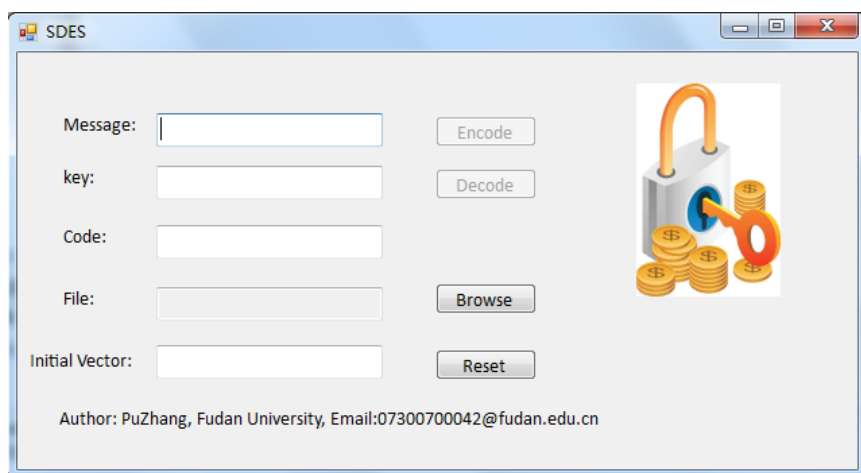
程序开发环境说明

在本程序的开发过程中，我使用了 Visual Studio2010 开发工具，采用了 C#开发语言，所以如果想要使用本程序，请确保您的电脑上有.NET Framework 4.0 的环境。

程序功能说明

本程序采用了图形界面，所以操作简单，使用方便。如下图所示，程序界面中有三个可以编辑的文本框，用户可以向其中输入相应的明文串，密文串或者密钥。注意，此处三种输入都是采用 0 和 1 组成的字符串来代表其实际的二进制形式输入的，这样一方面方便用户输入，另一方面方便用户查看输出结果。

同时，程序还可以对文件进行加密或者解密，只需要单击 Browse 按钮，选中想要加密或解密的文件（注意，此处文件是二进制形式），然后输入密钥，就可以对文件进行加密（Encode）或者解密（Decode）操作了，在对文件进行加密的时候，还需要提供 Initial Vector，作为 CBC 模式的 DES 的初始向量，每次在进行加密或者解密的时候都可以改变，同样 Initial Vector 也是采用 0 和 1 字符串组成的二进制串序列输入。程序面板上的 Reset 按钮可以将程序的状态变回原始状态，建议每次加密之前先点击 Reset 按钮，将程序初始化一下。

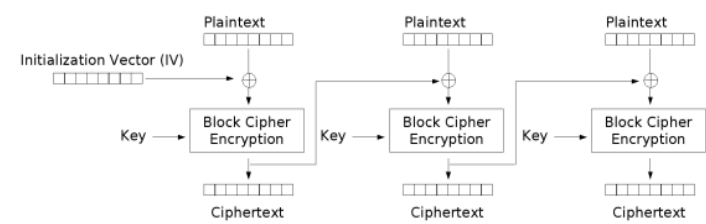


程序设计思想

在本程序设计中，一个非常重要的难关就是，计算机中的程序都是以 byte 形式存储的，但是在本算法中，所用的数据有 2 bits 形式存储的，有 4 bits 形式存储的，还有 8 bits 形式存储的。数据在这些存储形式中进行转换的时候会有不少麻烦。我将这些转换过程用调用子函数的形式实现，使得调用过程显得简洁。关于 CBC 模式教材上有详细的介绍，另外，SDES 算法，课件上也有详细的流程图，所以整个程序设计起来还是相当容易的。我的程序代码中有非常详细的注释，描述了整个程序的设计思路，在此不再重复。

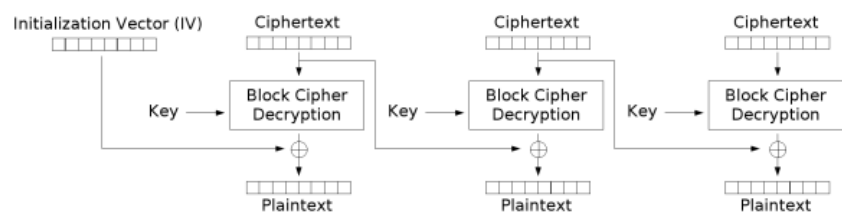
另附 CBC 的加密和解密过程示意图。

CBC 的加密过程示意图



Cipher Block Chaining (CBC) mode encryption

CBC 解密过程示意图



Cipher Block Chaining (CBC) mode decryption