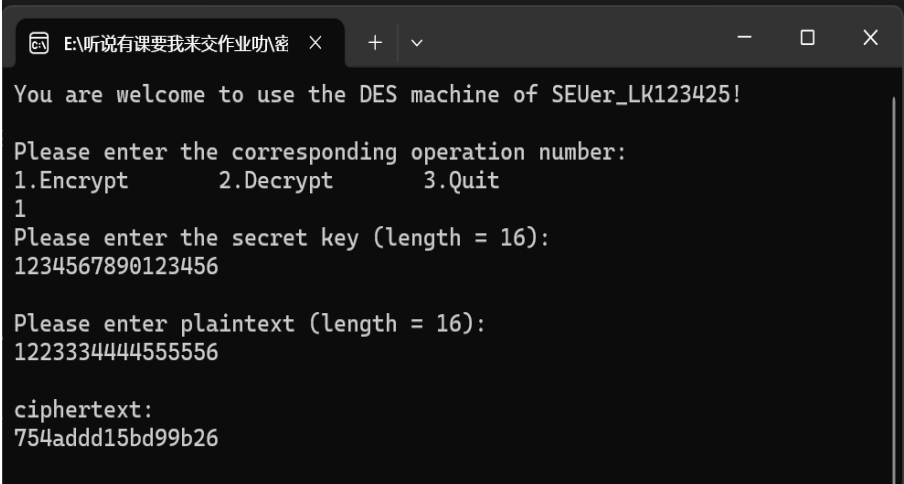


密码学实验一、 数据加密标准(DES)实验报告

班级 572221 学号 LK123425 姓名 黄睿扬

实验目的	1. 掌握 DES 结构，包括初始置换、轮结构、密钥生成、加解密； 2. 利用 C、C++、Java 实现 DES 算法
实验要求	1. 提交实验报告； 2. 提交实验代码
实验内容	1. 实现 DES 轮密钥生成； 2. 实现 DES 加密； 3. 实现 DES 解密； 4. 展示实验结果
实验环境	系统：Windows 11 （64 位） 处理器：AMD Ryzen9 7945HX（16 核） IDE：Visual Studio 2022 语言：C++、C 语言 环境：MinGW
实验步骤	<p>一、构建 DES 类</p> <ol style="list-style-type: none">1. 定义密钥扩展函数 <code>set_key</code>。2. 定义加密变换函数 <code>en_transform</code> 和解密变换函数 <code>de_transform</code>。3. 定义存放加密的子密钥 <code>enkey</code> 和存放解密的子密钥 <code>dekey</code>4. 完成对初置换表、逆置换表、E 表、置换选择表、置换选择 1、置换选择 2、密钥位移（左移次数）和 S 盒的定义。 <p>二、生成 DES 轮密钥</p> <ol style="list-style-type: none">1. 用 PC_1 表置换：去掉 64 bit 密钥 <code>k</code> 中的 8 个奇偶校验位，并对其余 56 位打乱排列。置换完成后，同样将密钥分成左右两部分各 28 bit。2. 循环移位：在第 <code>n</code> 轮分别对上一轮（<code>n-1</code> 轮）进行循环左移，所移的位数为 1 位或者 2 位，取决于 <code>n</code> 的值，其中当 <code>n=1,2,9,16</code> 时左移 1 位，其它左移 2 位。3. 置换选择 2：将每轮移位后的左右两部分拼接，然后由置换选择 2 表进行置换，生成 16 轮 48 比特轮密钥，用数组存储，以便解密使用。 <p>三、DES 加密</p> <ol style="list-style-type: none">1. 初始置换：依据初始置换表对 64 比特明文进行初始置换，然后分为左右两半 <code>larr</code> 和 <code>rarr</code>。2. 右拓展：由给定的选择扩展函数可以将 <code>rarr</code> 扩展为 48 比特。

	<ol style="list-style-type: none">3. 密钥异或：将经过拓展的 <code>rarr</code> 与该轮密钥进行异或4. S 盒代换：把比特串分为 8 组，一组 6 bit，分别对每一组进行 S 盒代换。经过 S 盒，每一组由 6 bit 缩减为 4 bit，总共即 32 比特。5. P 置换：P 为固定置换，将经过 S 盒变换得到的 32 bit 进行一个置换操作。6. 左右异或：经过 P 置换的 32 比特与 <code>larr</code> 异或，生成下一轮的 R。该轮初始 R 成为下一轮的 <code>larr</code>。7. 循环步骤 2-6 共 16 轮，然后左右交换，经过逆初始置换后得到 64bit 密文，加密完成。 <p>四、DES 解密</p> <p>使用加密同样的算法，输入为密文，每轮密钥倒序使用，输出结果即为明文。</p> <p>五、实验</p> <ol style="list-style-type: none">1. 定义 <code>main</code> 函数。2. 实例化类 DES 的对象 <code>mydes</code>。3. 分别调用加密函数 <code>en_transform</code> 和解密函数 <code>de_transform</code> 完成加解密操作。
实验结果	<ol style="list-style-type: none">1. 选择选项“1”。2. 设置密钥为“1234567890123456”。3. 设输入明文“1223334444555556”。4. 选择选项“2”。5. 输入密钥。6. 输入密文。7. 解密得到明文。 <p>运行结果如下：</p> 

You are welcome to use the DES machine of SEUer_LK123425!

Please enter the corresponding operation number:

1.Encrypt 2.Decrypt 3.Quit

2

Please enter the secret key (length = 16):

1234567890123456

Please enter the ciphertext (length = 16):

754add15bd99b26

plaintext:

1223334444555556