**深 圳 大 学 实 验 报 告**

**课程名称：­ 计算机安全导论**

**实验项目名称­： 对称密码实验**

**学院： 计算机与软件学院**

**专业： 计算机科学与技术**

**指导教师： 林秋镇**

**报告人： 学号： 班级：**

**实验时间： 2024年9月18日**

**实验报告提交时间： 2024年10月8日**

**教务部制**

|  |
| --- |
| 实验目的与要求：   1. 理解对称密码体制和分组密码算法的基本思想 2. 理解古典加密算法、DES、AES的基本原理，分析其安全强度关系、运行复杂度 3. 实现3DES的加解密过程 4. 针对各种文件（word、txt、mp3、jpg）进行3DES加解密操作 |
| 实验环境：  Microsoft Visual Studio 2005等 |
| 实验原理：  3DES（三重数据加密算法）是一种对称密钥加密算法，它基于DES（数据加密标准）算法。3DES通过应用三次DES加密过程来提高安全性。   1. 密钥生成   使用3DES，一般需要3个不同密钥，但也可以在E-D-E序列下使用2个密钥：  ***C* = *EK1*(*DK2*(*EK1*(*M*)))**  在安全上加密和解密是等效的。  ，相当于单个DES。  采用三个密钥的3DES的加密过程如下所示：  ***C* = *EK3*(*DK2*(*EK1*(*M*)))**  解密过程仅仅是使用相反的密钥顺序进行操作：  ***M* = *DK1*(*EK2*(*DK3*(*C*)))**     1. 加密过程：      * 初始置换：将64位的明文输入进行初始置换，打乱数据的排列。 * 子密钥生成：使用密钥生成算法从主密钥中生成16个子密钥，每个子密钥用于一轮加密。 * 16轮加密：明文通过16轮的Feistel结构进行加密，每轮包括以下步骤：   + 输入：将前一轮的输出分为两个32比特的部分，通常称为Li（左半部分）和Ri-1（右半部分）。   + 扩展运算E：对右半部分Ri-1进行扩展运算，将其扩展到48比特。扩展运算通常包括将32比特的数据通过特定的规则扩展到48比特，以便与子密钥进行异或操作。   + 子密钥K：将扩展后的数据与该轮的子密钥进行异或操作。子密钥是通过密钥调度算法从主密钥中派生出来的。   + 压缩运算S：对上一步的输出进行压缩运算，通常包括S盒（替代盒）的置换。这一步的目的是引入非线性，增加算法的复杂度和安全性。   + 置换运算P：对压缩运算的结果进行置换，将48比特的数据重新排列。   + 异或运算：将置换后的数据与左半部分Li进行异或操作。   + 输出：将上一步的异或结果作为新的右半部分Ri，将原来的右半部分Ri-1作为新的左半部分Li+1。   + 迭代：重复上述步骤，直到完成16轮的加密。      * 左右交换：16轮结束后，将两部分数据交换位置。 * 逆初始置换：最后进行逆初始置换，恢复数据的原始排列。      1. 解密过程：   解密过程与加密过程类似，但子密钥的使用顺序相反。解密时，先使用第16轮的子密钥，然后是第15轮的，依此类推，直到第1轮。  密码分组链接模式是消息被切分成多个分组,在加密操作时每一个明文分组与前面密文分组相链接，使得同一明文分组将会产生不同的密文分组，以此来对明文进行整体加密。   1. 加密   ***Ci* = *EK*(*Pi* XOR *Ci*-1)**  在CBC模式中，每个明文块在加密前会与前一个密文块进行异或操作，第一个块与初始化向量（IV）异或。     1. 解密   ***Pi* = *DK*(*Ci*)XOR *Ci*-1**  在解密时，每个密文块在解密后会与前一个密文块进行异或操作，以恢复原始的明文块。 |
| 实验内容：   1. 采用自己熟悉的编程语言实现3DES加密算法 2. 将编写的3DES用于加密各种文件（word、txt、mp3、jpg），并能成功解密 |
| 实验步骤与结果：   1. 3DES加密算法的实现 2. 初始化代码所需的各种矩阵              1. 子密钥生成   以下代码实现了子密钥生成。首先，使用初始置换规则（PC-1）将主密钥转换为56位，接着将其分为两个28位的部分C和D。然后，根据预定义的移位规则，对C和D进行左循环移位，合并后更新为新的56位密钥。最后，通过另一置换规则（PC-2）从更新后的密钥中提取出当前的48位子密钥，并将其存储在子密钥数组中，重复这一过程直到生成所有16个子密钥。     1. 轮函数实现   以下代码实现了加密算法中的轮函数F，主要流程包括扩展输入的32位数据到48位，随后与48位的子密钥进行异或运算。接着，利用S盒将扩展后的48位数据压缩回32位。在压缩过程中，先计算行和列以获取S盒的值，并将该值转化为4位二进制，最后根据P盒对压缩后的数据进行置换，返回处理后的32位结果。     1. DES加密   以下代码实现了数据加密标准（DES）的加密过程。首先，它生成16个子密钥，并对输入的64位明文进行初始置换。接着，将明文分割为左右两部分，进入16轮加密。在每轮中，右半部分与通过轮函数F和相应子密钥计算得出的值进行异或运算，左半部分则被更新为原来的右半部分。完成所有轮次后，左右两部分交换位置，并对结果进行逆初始置换，最终返回加密后的密文。     1. DES解密   以下代码实现了数据加密标准（DES）的解密过程。它首先生成16个子密钥，并对输入的64位密文进行初始置换，然后将密文分为左右两部分。在16轮解密过程中，右半部分与轮函数F和反向子密钥的异或结果进行更新，左半部分则被更新为原来的右半部分。最后，左右两部分交换位置，并对结果进行逆初始置换，最终返回解密后的明文。     1. 3DSE加密和解密   以下代码实现了三重数据加密标准（3DES）的加密和解密过程。在加密过程中，首先使用第一个密钥对明文进行DES加密，然后使用第二个密钥对得到的密文进行DES解密，最后再用第三个密钥进行DES加密，最终得到密文。在解密过程中，顺序则反向进行：首先用第三个密钥解密密文，再用第二个密钥加密得到的结果，最后用第一个密钥解密，最终得到明文。这种方法增强了安全性，因为它结合了三次DES操作。     1. 文件的比特流读取和写入   以下代码实现了将文件内容以64位比特读取和写入的功能。在readBitsFromFile函数中，首先从文件读取8个字节（64位），然后逐位将这些字节转换为bitset<64>格式的比特集合并返回。在writeBitsToFile函数中，64位比特被分组为字节，每8位组成一个字节，写入到指定的文件中。通过这种方式，可以有效地在文件和比特表示之间进行转换。     1. 密码分组链接模式下加密   以下代码实现了基于密码分组链接模式（CBC）的文件加密功能。首先，打开输入文件和输出文件。如果成功打开，则链块C初始化为初始向量（IV），读取输入文件中的数据块（64位比特），并与链块C进行异或操作，然后通过3DES算法加密该结果。加密后的结果更新链块C，用于下一个数据块的加密。这个过程持续进行，直到文件结束，最终将所有加密结果写入输出文件中。     1. 密码分组链接模式下解密   以下代码实现了基于密码分组链接模式（CBC）的多线程解密功能。首先，打开输入和输出文件。如果成功打开，则不断读取64位比特块，利用处理器的数量来并行解密这些块。每个解密工作由一个线程执行，使用3DES解密算法并结合之前的密文块进行异或操作。解密结果通过互斥量安全地存储到共享向量中。所有线程完成后，解密结果被写入输出文件，接着更新链块C和清空临时存储，直到文件读取完成。         1. 密钥和初始向量的生成   采用随机数生成64位的密钥和初始向量。     1. 3DES用于加密各种文件（word、txt、mp3、jpg） 2. 加密解密word文件   代码：    加密前：  密文：    解密后：   1. 加密解密txt文件   代码：    加密前：  密文：    解密后：   1. 加密解密mp3文件   代码：    加密前：  密文：    解密后：     1. 加密解密jpg文件   代码：    加密前：  密文：    解密后： |
| 实验结论：  在本次实验中，我深入理解了对称密码体制和分组密码算法的基本思想，尤其是3DES的加解密过程。在文件加解密方面，我成功地将3DES应用于多种格式（如word、txt、mp3、jpg），并且在解密过程中确保了数据的完整性。这表明3DES能够适应不同类型的文件，但在处理效率上依然面临挑战。  3DES相比DES的优势在于，3DES进行了3次DES的加密操作，显著增加了密钥空间，从56位扩展到168位（在使用三个不同密钥的情况下），使得对暴力破解的抵抗能力更强。  但与AES相比，3DES的安全性和效率均显得逊色。AES支持更大的块大小和更灵活的密钥长度，使用了更复杂的数学工具，同时在性能上也更优越，运行时间更短。  扩展性上，3DES的可扩展性强，适用于多种文件类型（如文本、音频、图像等），可以实现对各种格式的加解密，同时可执行x次DES加密，变为xDES。 |
| 指导教师批阅意见：  成绩评定：  指导教师签字：  年 月 日 |
| 备注： |

注：1、报告内的项目或内容设置，可根据实际情况加以调整和补充。

2、教师批改学生实验报告时间应在学生提交实验报告时间后10日内。