**《密码学》课程设计实验报告**

实验序号：03　　　　　　　　　　实验项目名称：分组密码工作模式

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 学　　号 |  | 姓　　名 |  | 专业、班 | | 21信安 |
| 实验地点 | C202 | 指导教师 | 余荣威 | 时间 | | 2023.12.8 |
| 1. 实验目的及要求   教学目的：   1. 掌握分组密码的基本概念； 2. 掌握DES、AES、SMS4密码算法； 3. 了解分组密码DES、AES、SMS4的安全性； 4. 掌握分组密码常用工作模式及其特点； 5. 熟悉分组密码的应用。   实验要求：   1. 掌握分组密码的ECB、CBC、OFB、CFB、CTR等常用工作模式； 2. 掌握分组密码的短块加密技术； 3. 熟悉分组密码各工作模式的（数据掩盖、错误传播、效率等）特点； 4. 利用分组密码工作模式和短块处理技术实现任意长度输入的加密与解密。   二、实验设备（环境）及要求  Windows操作系统，高级语言开发环境  三、实验内容与步骤  1. 分组密码的常用工作模式  （1）电码本模式ECB（教材 p124 式3-76）  （2）密文链接模式CBC（教材 p125 图3-30、31）  （3）输出反馈模式OFB（教材 p127 图3-32）  （4）密文反馈模式CFB（教材 p128 图3-33）  （5）X CBC模式（教材 p128 式3-81-83）  （6）计数器模式（教材 p128 式3-84、85）  2. 分组密码的短块处理技术  （1）填充法  参考X CBC模式的填充方案  （2）序列密码加密法（教材 p130 图3-34）  （3）密文挪用技术（教材 p130 图3-35）  3. 各工作模式的特点比较  设明文*M*=（*M*1 ，*M*2 ，…，*M*n ），相应的密文*C*=( *C*1 ，*C*2 ，…，*C*n )。试完成下列实验，总结各工作模式的特点，并完成表格1：  （1）选择输入消息*M*i ＝*M*j ，判断是否满足*C*i =*C*j ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。  （2）选择篡改输入明文中的某个分块*M*i ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。  （3）选择篡改输入密文中的某个分块*C*i ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。  （4）比较不同的工作模式对于输入消息长度的要求。  （5）比较不同的工作模式的执行效率。  4. 短块处理技术的比较  设明文实际长度不是分组长度的整倍数，试使用填充法、序列密码加密法、密文挪用技术进行处理。总结这三种方法的特点，并完成表格2：  （1）是否造成短块数据扩张；  （2）试分析三种方案的安全性（提示：假设攻击者进行选择明文攻击）  四、实验结果与数据处理  **4.1分组密码的常用工作模式**  表1：各工作模式的特点   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 工作模式 | 电码本模式ECB | 明密文链接模式 | 密文链接模式CBC | 输出反馈模式OFB | 密文反馈模式CFB | XCBC模式 | 计数器模式CTR | | 能否掩盖数据模式 | 否 | 能 | 能 | 能 | 能 | 能 | 能 | | 加密错误传播无界 | 有界 | 无界 | 无界 | 有界 | 无界 | 无界 | 有界 | | 解密错误传播无界 | 有界 | 无界 | 有界 | 有界 | 无界 | 无界 | 有界 | | 是否改变消息长度 | 不能 | 不能 | 不能 | 不能 | 不能 | 不能 | 不能 | | 能否处理消息短块 | 不能 | 不能 | 不能 | 能 | 能 | 能 | 能 | | 执行速度 | 最快 | 较慢 | 较慢 | 较快 | 较快 | 最慢 | 快 |   **4.2各工作模式的特点比较**  本实验在AES下实现  **4.2.1 ECB**    （1）选择输入消息Mi ＝Mj ，判断是否满足Ci =Cj ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看结果    可以看到ECB不能掩盖明文的数据模式  （2）选择篡改输入明文中的某个分块Mi ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看结果    ECB模式下，明文被分成固定大小的块，并且每个块都独立地进行加密，因此加密错误传播有界。  （3）选择篡改输入密文中的某个分块Ci ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看结果    可以看到密文被修改，运行结果说明在ECB解密过程中，如果某个密文块发生错误，那么仅仅会影响对应的明文块，而不会波及到其他部分。这是因为每个密文块都是独立解密的，解密一个块不依赖于其他块，因此错误传播有界。  （4）比较不同的工作模式对于输入消息长度的要求。    在ECB模式中，输入消息的长度要求是分组长度的整数倍。每个明文块都要被分割成大小相同的块，并独立加密。因此，如果明文的长度不是分组长度的整数倍，需要进行填充以满足这一要求。  （5）比较不同的工作模式的执行效率。    运行结果    可以看到ECB运行速度非常快，因为每个块的加密是独立的。  **4.2.2 CBC**    （1）选择输入消息*M*i ＝*M*j ，判断是否满足*C*i =*C*j ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看运行结果    可以看到CBC可以掩盖明文的数据模式  （2）选择篡改输入明文中的某个分块*M*i ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看运行结果    在只更改了明文的第一位的情况下，可以看到密文的整体都发生了错误，得出加密错误传播无界  （3）选择篡改输入密文中的某个分块*C*i ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看运行结果    可以看到我更改了密文第16位，导致明文的M1出错，但是M2正常，表明解密错误传播是有界的  （4）比较不同的工作模式对于输入消息长度的要求。  在CBC模式下，消息输入的长度要求是分组长度的整数倍。在上述代码中，AES分组长度为16字节（128位），因此明文的长度应该是16字节的整数倍。  如果明文的长度不是分组长度的整数倍，就需要进行填充操作，以满足整数倍的要求。在这里，本实验使用的是PKCS7填充方式，即用需要填充的字节值填充到需要填充的长度。  pkcs7padding函数对明文进行填充，而pkcs7unpadding函数对解密后的数据进行去除填充操作。这样可以确保输入的消息长度符合CBC模式的要求，实现的代码如下：      （5）比较不同的工作模式的执行效率。    查看运行结果    可以看到运行时间还是比较长的  **4.2.3 OFB**  将一个分组密码转换为一个密钥序列产生器，从而可以实现用分组密码按流密码的方式进行加解密。      （1）选择输入消息Mi ＝Mj ，判断是否满足Ci =Cj ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看运行结果    OFB可以掩盖明文中的数据模式。  （2）选择篡改输入明文中的某个分块Mi ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看运行结果    可以看到对前面几位明文的篡改并未影响到后续的密文，加密错误传播有界  （3）选择篡改输入密文中的某个分块Ci ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看运行结果    改动密文一位，不影响后面的明文，解密错误传播有界  （4）比较不同的工作模式对于输入消息长度的要求。  由于OFB模式通过生成随机比特流（种子R0）与明文进行异或操作，因此，OFB模式对明文的长度没有限制要求。消息的长度可以是任意的，不必是分组长度的整数倍。  （5）比较不同的工作模式的执行效率。    查看运行结果    可以看到OFB运行较快  **4.2.4 CFB**  与OFB不同的是，CFB是把密文反馈到移位寄存器      （1）选择输入消息Mi ＝Mj ，判断是否满足Ci =Cj ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看运行结果    可以看到CFB可以掩盖明文的数据模式  （2）选择篡改输入明文中的某个分块Mi ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看运行结果    可以看到我只更改了明文的几位，整体的密文却发生了改变，证明错误传播无界  （3）选择篡改输入密文中的某个分块Ci ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看运行结果    解密的错误传播无界  （4）比较不同的工作模式对于输入消息长度的要求。  与OFB类似，CFB模式对明文的长度没有限制要求。消息的长度可以是任意的，不必是分组长度的整数倍。  （5）比较不同的工作模式的执行效率。      查看运行结果    可以看到CFB加密时间略慢于OFB，解密时间稍微长了一些，和其工作模式有较为紧密的关联  **4.2.5 CTR**    （1）选择输入消息Mi ＝Mj ，判断是否满足Ci =Cj ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看运行结果    CTR可以掩盖明文的数据格式  （2）选择篡改输入明文中的某个分块Mi ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看运行结果    修改明文前几位，不影响后续的密文，加密传播错误有界  （3）选择篡改输入密文中的某个分块Ci ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看运行结果    可以看到更改了密文，解密的明文后面几位并未发生变化，即解密错误传播有界  （4）比较不同的工作模式对于输入消息长度的要求。  CTR模式的输入信息长度可以是任意的，不必是分组长度的整数倍。这是因为CTR模式仅使用计数器和初始向量生成密钥流，可以逐块地对输入信息进行加密，无论输入信息的长度是多少。  （5）比较不同的工作模式的执行效率。    查看运行结果    可以看到CTR的加解密速度很快，优于上述几种（除ECB）  **4.2.6 XCBC**      （1）选择输入消息Mi ＝Mj ，判断是否满足Ci =Cj ？对于不同的工作模式分别进行上述实验，得出各工作模式是否能够掩盖明文中的数据模式的判断。    查看运行结果    可以看到XCBC可以掩盖明文的数据模式  （2）选择篡改输入明文中的某个分块Mi ，并将加密后的结果与正确的密文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有加密错误传播无界特性的判断。    查看运行结果    XCBC模式下加密错误传播有界  （3）选择篡改输入密文中的某个分块Ci ，并将解密后的结果与正确的明文之间进行对比。对于不同的工作模式分别进行上述实验，得出各工作模式是否具有解密错误传播无界特性的判断。    查看运行结果    可以看到解密错误传播无界  （4）比较不同的工作模式对于输入消息长度的要求。  XCBC是CBC工作模式的改进，XCBC不要求最后一个数据块是标准块，因为有填充，所以对于输入消息的长度没有要求，但是要传输填充长度信息。  （5）比较不同的工作模式的执行效率。    查看运行结果    可以看到XCBC的时间较慢  **4.3 短块加密**   |  |  |  |  | | --- | --- | --- | --- | | 短块处理方式 | 填充 | 序列密码加密 | 密文挪用 | | 短块数据扩张 | 是 | 是 | 否 | | 实现难度 | 易 | 适中 | 难 | | 安全性 | 弱 | 始终 | 强 |   五、分析与讨论  1.三种短块加密方法的安全性分析  （1）填充法  填充法是通过在明文的末尾添加额外的数据，使其长度成为分组长度的整数倍。常见的填充方案有PKCS#7和ISO/IEC 7816-4。填充法简单易实现，但可能导致短块数据扩张，即在原有明文长度的基础上增加一整个分组的长度。这样的话，攻击者可以根据密文长度判断明文的原始长度。  安全性分析：填充法的主要安全性问题在于可能泄漏明文的长度信息。攻击者可以通过观察密文长度的变化，推测出明文的长度。因此，在对安全性要求较高的场景中，可能需要采用其他更为安全的方案。  （2）序列密码加密法  序列密码加密法是一种使用密钥流对明文进行加密的方法。密钥流是一个与明文等长的比特序列，通过密钥和初始向量生成。由于是按比特进行加密，不需要进行分组填充，因此不会出现短块数据扩张的问题。  安全性分析：序列密码加密法的安全性与生成密钥流的算法和密钥管理密切相关。如果密钥流是伪随机的且不可预测的，那么该方案可以提供较高的安全性。但如果密钥流的生成存在问题，例如伪随机性不足，可能导致安全性降低。  （3）密文挪用技术  密文挪用技术是一种通过对密文进行重新排列或变换的方式，来处理明文长度不是分组长度整数倍的情况。这样可以避免短块数据扩张问题。一个常见的例子是使用流密码的密文挪用。  安全性分析：密文挪用技术的安全性也取决于具体的实现方式。如果重新排列或变换的过程是可逆的且与密钥相关，且没有明显的模式可循，那么该方案可以提供较高的安全性。  2.如何提升分组密码的工作效率  （1）并行加/解密：在现代硬件中，很多处理器都支持并行计算，可以利用这一特性，同时加密/解密多个分组。例如，在CBC模式中，可以同时处理多个分组的加密/解密，从而提高效率。  2. 内存对齐和数据对齐： 对于分组密码操作，内存对齐和数据对齐可以提高访问速度。确保数据结构和算法都能够充分利用处理器的缓存。  3. 预计算：对于一些可预测的计算，可以在加密/解密开始前进行预计算，从而减少实际加密/解密时的计算量。  4. 选择合适的分组大小： 在使用CTR模式时，选择合适的分组大小可以影响加密/解密效率。通常较大的分组大小会提高效率，但也要注意不要选择过大以避免安全问题。  需要注意的是，对于提升运行效率的优化，需要综合考虑具体的应用场景和安全性需求。在选择和实现优化策略时，应该确保不会牺牲系统的安全性。 | | | | | | |
| 六、教师评语  签名：  日期： | | | | | 成绩 | |