**《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 | | 18信安 |
| 实验地点 | 新珈楼B310实验室 | 指导教师 | 王后珍 | 时间 | | 2020.12.07 |
| 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  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 | 不能 | 能 | 能 | 能 | 能 | 能 | 能 | | 加密错误传播无界 | 否 | 是 | 是 | 否 | 是 | 是 | 否 | | 解密错误传播无界 | 否 | 是 | 否 | 否 | 是 | 否 | 否 | | 是否改变消息长度 | 否 | 否 | 否 | 否 | 否 | 否 | 否 | | 能否处理消息短块 | 不能 | 不能 | 不能 | 能 | 能 | 能 | 能 | | 执行速度 | 快 | 适中 | 适中 | 快 | 快 | 慢 | 快 |  |  |  |  |  | | --- | --- | --- | --- | | 短块处理方式 | 填充 | 序列密码加密 | 密文挪用 | | 短块数据扩张 | 会造成 | 会造成 | 不会造成 | | 实现难度 | 易 | 中 | 较难 | | 安全性 | 弱 | 若 | 强 |   ***分组工作模式具体说明***   * **电话本模式**   + 直接利用分组密码对明文的各分组进行加密   + 缺点  1. 不能解决短块问题 2. 容易暴露明文的数据模式。在计算机系统中，许多数据都具有某种固有的模式，这主要是由数据冗余和数据结构引起的。例如，各种计算机语言的语句和指令都十分有限，因为在程序中便表现为少量的语句和指令的大量重复    * 流程图      * **明密文链接模式**   + 设明文，相应的密文   + 特点     1. 加解密错误传播无界     2. 无法处理短块   + 流程图      * **密文链接模式**   + 由于明密文链接模式具有加解密错误传播无界的特性，而磁盘等文件通常希望错误传播有界，这时可采用密文链接模式   + 设明文，相应的密文   + 特点     1. 无法处理短块     2. 加密错误传播无界，解密错误传播有界 * **输出反馈模式**   + 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。   + 特点     1. 工作模式的安全性取决于分组密码本身的安全性     2. 可以解决短块加密     3. 无错误传播     4. 适用于加密冗余度较大的数据，例如语音和图像数据   + 流程图      * **密文反馈模式**   + 与输出反馈的工作原理基本相同，所不同的仅仅是反馈到移位寄存器的不是输出中的最右位，而是密文的位   + 流程图      * **X CBC**模式   + X CBC模式解决了CBC模式要求明文数据的长度是密码分组长度的整数倍的限制，可以处理任意长的数据   + 优点     1. 可以处理任意长度的数据     2. 适用于计算产生检测数据完整性的消息认证码MAC   + 缺点     1. 使用3个密钥，密钥的存储和加解密控制都比较麻烦     2. 接受双方需要共享填充的消息长度 * **CTR模式**   + 与密文反馈工作模式和输出反馈工作模式一样，把分组密码转换为序列密码，在本质上是利用分组密码产生密钥序列，按序列密码的方式进行加密   + 优点     1. 可并行，效率高     2. 适合任意长度的数据     3. 加解密速度快   + 缺点     1. 没有错误传播，不适用于数据完整性验证   + 流程图     五、分析与讨论   1. 分组密码不同的工作模式各有各的特点，例如有些工作模式需要处理短块，有些则不需要；有些模式具有错误传播无界的特性，有些则没有。这些特点通常需要与实际的应用场景相结合，而并没有绝对的优劣之分 2. 利用输出反馈模式可以将分组密码转换成一个密钥序列产生器，达到和序列密码相似的功能。 3. 在对某些结构化的数据进行加密时，我们可以通过链接技术消除数据固有的模式 | | | | | | |
| 六、教师评语  签名：  日期： | | | | | 成绩 | |