# 现代密码应用与分析实验

主要内容：现代密码（AES、DES）加解密；视频文件保护（机密、完整、消息认证）

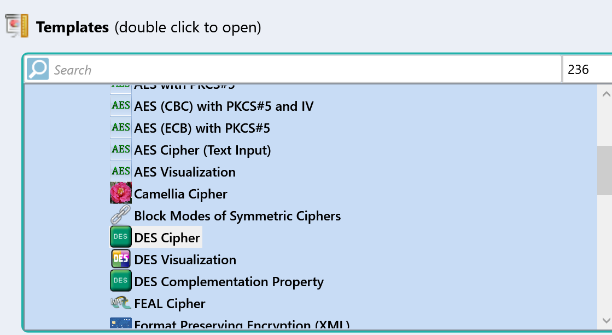
## **基于Cryptool的现代密码加解密与分析实验**

### 主要内容

1. DES、AES加密、解密实验、雪崩效应分析
2. 自行设计基于Feistel结构的分组密码，雪崩效应分析

### 利用向导选项中DES密码加密，并对三则密文分别解密

1. 菜单选项位置



1. 设置加密参数

• 模式

• ECB、CBC、CFB、OFB

• 密钥

• 明文字符串

• 8英文字符、16英文字符、任意长字符串

1. 设置解密参数

• 模式

• 与加密对应的设置

• 密钥

• 与加密对应的设置

• 明文字符串

• 与加密对应的设置

1. 记录加密、解密、结果屏幕截图
2. 填写加密、解密情况汇总表

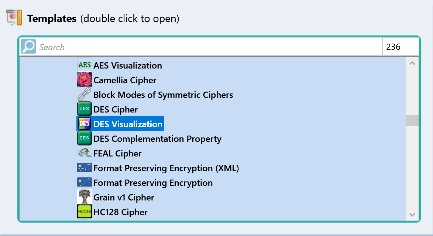
• 不同模式下记录加密明文、密文、密钥、明文长度、密文长度、密钥长度

• 比较不同明文（微小区别）产生的密文有多少比特或字节不同

• 比较不同明文长度时，密文长度的区别，以及与密文长度与明文长度是否一致

• 比较相同明文在不同模式下产生的密文的区别

1. 以8英文字符为例，熟悉DES加密过程，并参看各轮加密情况



• 注意调整模块配置为：接收字符串为输入

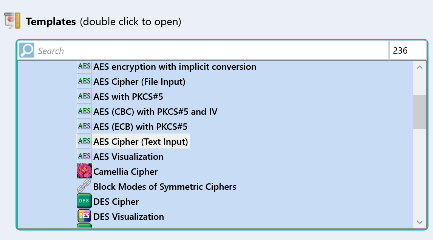
• 记录第1轮、第8轮、第16轮的输入比特（分为L、R）

• 比较并记录第8轮与第1轮相比，发生改变的比特数量

• 比较并记录第16轮与第1轮相比，发生改变的比特数量

### 利用向导选项中AES密码加密，并对三则密文分别解密

1. 菜单选项位置



1. 设置加密参数

• 模式

• ECB、CBC、CFB、OFB

• 密钥长度

• 128、192、256

• 密钥

• 明文字符串

• 8英文字符、16英文字符、任意长字符串

1. 设置解密参数

• 模式

• 与加密对应的设置

• 密钥长度

• 与加密对应的设置

• 密钥

• 与加密对应的设置

• 明文字符串

• 与加密对应的设置

1. 记录加密、解密、分析的结果屏幕截图
2. 填写加密、解密、分析情况汇总表

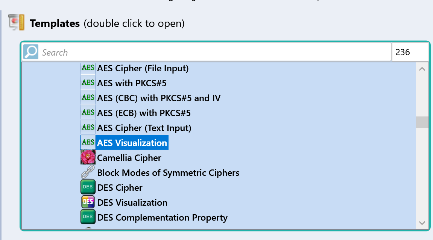
• 不同模式下记录加密明文、密文、密钥、明文长度、密文长度、密钥长度

• 比较不同明文（微小区别）产生的密文有多少比特或字节不同

• 比较不同明文长度时，密文长度的区别，以及与密文长度与明文长度是否一致

• 比较相同明文在不同模式下产生的密文的区别

1. （选做）以16英文字符为例，熟悉AES加密过程，并参看各轮加密情况



• 注意调整模块配置为：接收字符串为输入

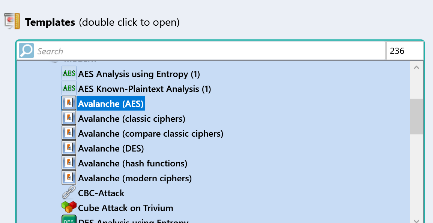
• 记录加密第1轮、第10轮的输入状态矩阵

• 比较并记录第10轮与第1轮相比，发生改变的比特数量

### 利用模板选项查看比较雪崩效应效果

1. AES

• 菜单选项位置



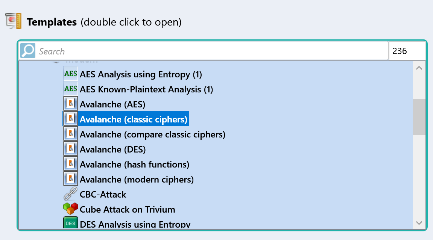
• 固定选取一个密钥，随机选取三组明文，进行雪崩效应实验

• 按照instruction操作，注意每次调整明文时仅修改一个字符或比特

• 记录修改前后的明文比特序列，记录每一轮次输出的密文值，以及雪崩效应影响的比特位占比

1. Caesar

• 菜单选项位置



• 按照instruction操作，注意每次调整明文时仅修改一个字符

• 记录修改前后的明文序列，记录密文值，以及雪崩效应影响的比特位占比

1. 比较AES和Caesar在雪崩效应上的区别

### 算法设计实验

基于Feistel结构自行设计一个分组算法，并给出雪崩效应的实例（即给出一个随机的输入，改变1比特后，追踪所有各处理环节及轮次改变的比特数量比例）。

### 现代密码加解密与分析实验报告

* 标题

• 实验名称、班级、姓名、学号

* 利用向导选项中DES密码加密，并对三则密文分别解密

• 简述实验步骤

• 屏幕截图

• 汇总表

• 分析与结论

* 利用向导选项中AES密码加密，并对三则密文分别解密

• 简述实验步骤

• 屏幕截图

• 汇总表

• 分析与结论

* 利用模板选项查看比较雪崩效应效果

• 简述实验步骤

• 屏幕截图

• 汇总表

• 分析与结论

* 基于Feistel结构自行设计一个分组算法，并给出雪崩效应的实例（即给出一个随机的输入，改变1比特后，追踪所有各处理环节及轮次改变的比特数量比例）

• 简述实验步骤

• 屏幕截图

• 汇总表

• 分析与结论

## **离线内容保护（面向点播）**

开发工具不限

### 任务简介

* 主题

• 单一程序实现对TS流媒体文件的离线加密、解密，并将结果保存到文件

* 目标

• 实现加密、解密操作的选择；实现对选定的TS流媒体文件利用指定的密钥和算法进行加解密

* 基本要求

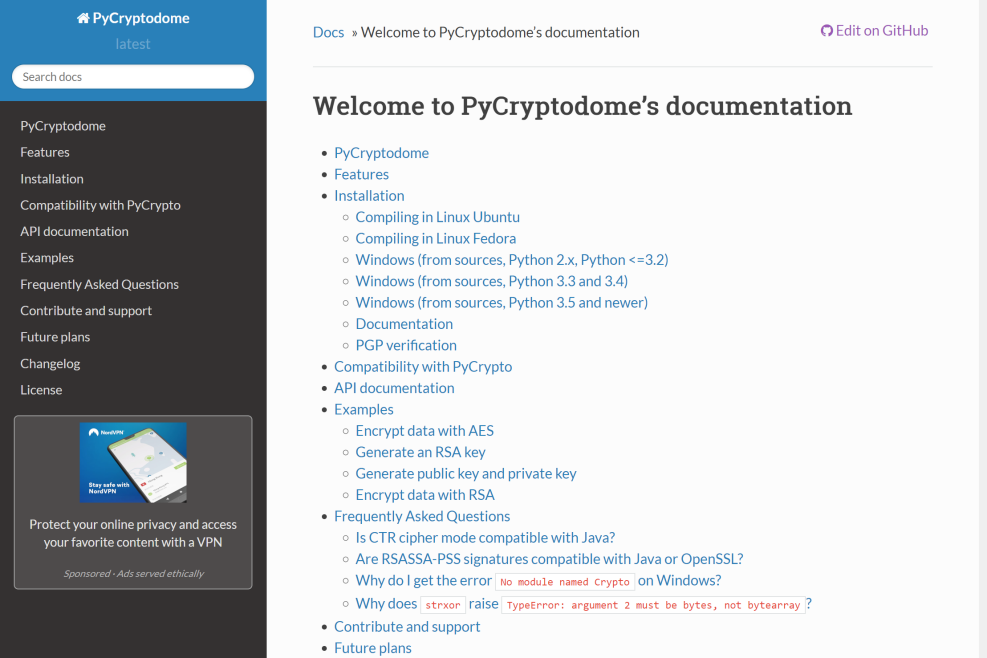
• 要求对使用DES算法加密时去除弱密钥和半弱密钥；要求加密后的密文和解密后的明文放到用户指定的的文件中

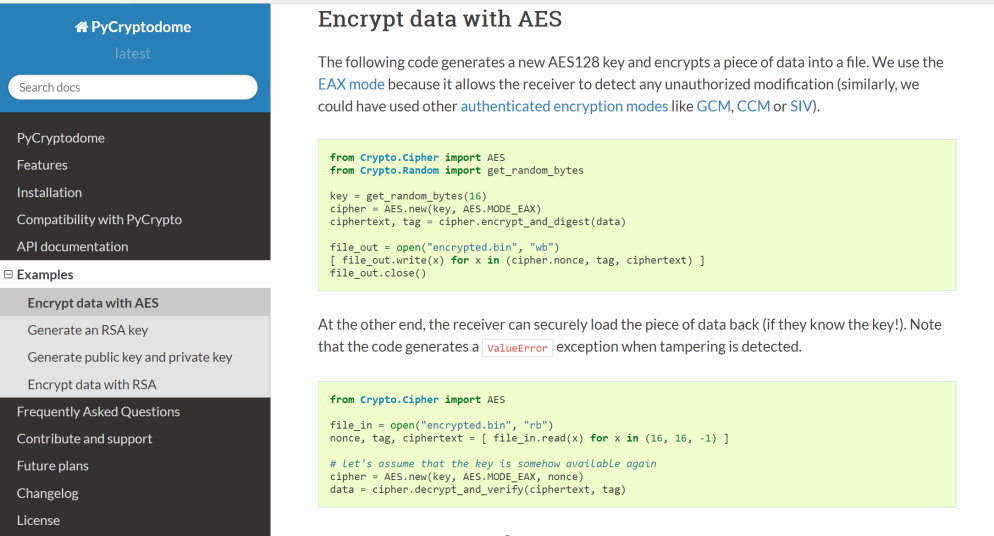
* 强调对现代密码典型分组算法的理解和基本使用、通过扩展选择要求达到对常见媒体封装格式TS的了解

### 基本步骤

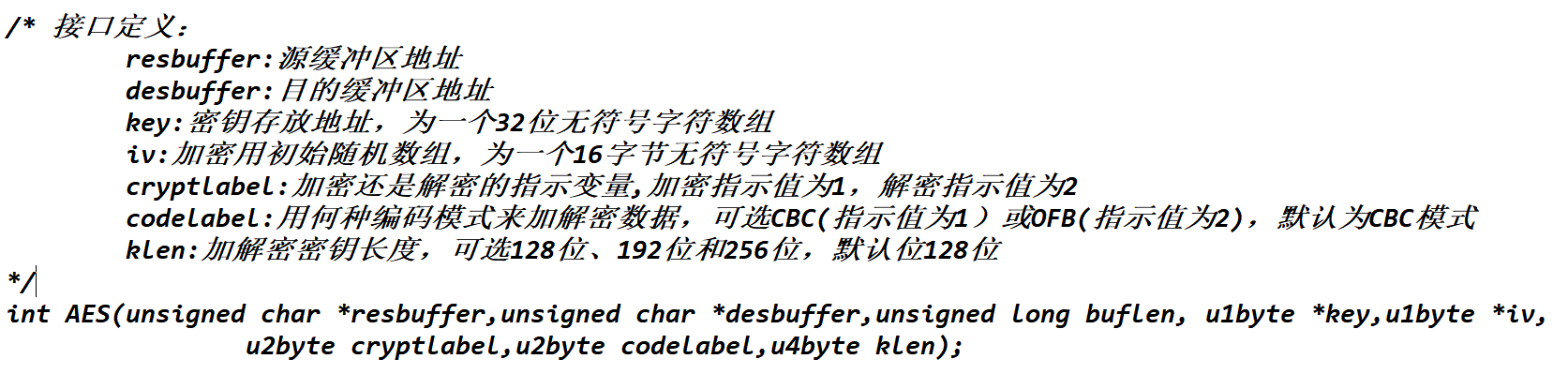
1. 工程的建立、文件的读取与写入、交互UI的设计与实现
2. 密码库的准备、密钥的准备、算法的准备

* pip install pycryptodome
* 了解基本使用方法
  + <https://www.pycryptodome.org/en/latest/>





* C/C++：AES算法源代码
* 了解AES算法与工作模式接口定义(AESmode.h)



1. 加密模块的设计实现
2. 解密模块的设计实现
3. 离线内容保护系统的运行与调试
4. 扩展内容（选作）

* 支持对TS流媒体数据的解析、加密、解密；要求每个TS块的头部不加密
* 加密时利用随机数生成器生成密钥、以BASE64编码的方式存储到密钥文件中；解密时读取BASE64编码的密钥文件得到主密钥用于解密操作

1. 实验报告要求

* 给出加密、解密详细流程图
* 给出执行结果截图
* 给出代码工程压缩包

## **在线内容保护（面向直播）（可选）**

开发工具不限

### 任务简介

* 主题

• 单一程序实现对UDP协议TS流媒体内容的实时接收、加密、解密，并将结果保存到文件

* 目标

• 实现对加密、解密操作、运行模式的选择；基于UDP协议接收来自网络的实时TS流媒体内容；对接收到的流媒体片段按照指定的运行模式进行加密、解密

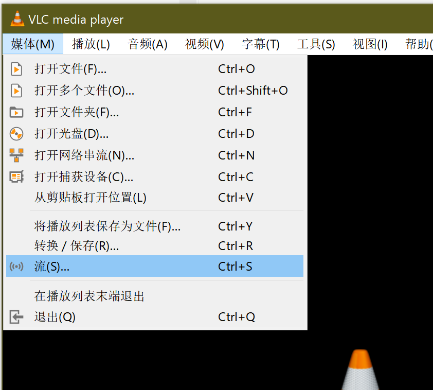
* 基本要求

• 要求对使用DES算法加密要去除弱密钥、半弱密钥；对使用AES算法要允许用户选择3中密钥长度；要求加密后的密文和解密的明文保存到用户指定的文件中

* 强调对现代密码分组密码运行模式的理解和基本使用、对流媒体实时接收和处理基本方法的了解

### 基本步骤

1. 利用VLC搭建基于UDP的基本的流媒体发送、接收、存储的测试环境



1. 工程的建立、UDP协议数据的读取与缓冲；文件的写入、交互UI的设计与实现
2. 密码库的准备、密钥的准备、算法的准备
3. 密码运行模式的设计实现
4. 加密模块的设计实现
5. 解密模块的设计实现
6. 在线内容保护系统的运行与调试

### 扩展内容（可选）

* 支持对TS流媒体数据的解析、加密、解密；要求每个TS块的头部不加密
* 加密时利用随机数生成器生成密钥、以BASE64编码的方式存储到密钥文件中；解密时读取BASE64编码的密钥文件得到主密钥用于解密操作

### 实验报告要求

* 给出加密、解密详细流程图
* 给出执行结果截图
* 给出代码工程压缩包