**ICQ题目设计说明书**

出题人：ｉ春秋

出题时间：2018/12/17

文档变更记录

（A：增加、M：修改、D：删除）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 状态 | 参与者 | 日期 | 描述 |
| V1.0 | A | 鸽子 | 2016.08.05 | 初稿 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1 题目设计 4](#_Toc482712096)

[1.1 设计思路 4](#_Toc482712097)

[1.2 题目难度和分值估计 4](#_Toc482712098)

[1.3 题目制作方法 4](#_Toc482712099)

[1.4 题目部署方法 6](#_Toc482712100)

[1.4.1 题目运行环境 6](#_Toc482712101)

[1.4.2 题目部署详细过程 6](#_Toc482712102)

[1.4.3 其他说明 6](#_Toc482712103)

[1.5 关键技术及解题文档 7](#_Toc482712104)

[1.5.1 关键技术 7](#_Toc482712105)

[1.5.2 解题思路 7](#_Toc482712106)

[1.5.3 解题步骤 7](#_Toc482712107)

[1.5.4 竞赛结果提交 15](#_Toc482712108)

[2 附件 15](#_Toc482712109)

[2.1 附件1：题目部署相关 15](#_Toc482712110)

[2.2 附件2：题目解题相关 15](#_Toc482712111)

[2.3 附件3：题目虚拟机 15](#_Toc482712112)

[3 附件 15](#_Toc482712113)

[3.1 附件1：服务检测脚本 15](#_Toc482712114)

[3.2 附件2：题目部署脚本 15](#_Toc482712115)

题目设计

## 设计思路

赛题出题思路主要围绕着USB协议数据分析，编程能力考察，隐写术的认知考点等知识点进行，难点是U盘和键盘产生的USB流量的分析以及根据题目需求编写辅助脚本。

## 题目难度和分值估计

赛题涉及到密码算法分析，逆向算法得到基本原理，Hill密码破解只是最后一个步骤

|  |  |
| --- | --- |
| 题目ID | ~~不需要填写~~ |
| 题目名称 | WHAT |
| 分值 | 500 |
| 类型 | Crypto |
| 题目描述 | 直接提供附件地址 |
| Flag | LANCET{Do\_You\_Know\_Hills\_Secret} |

## 题目制作方法

第一步:调用encrypt.py

调用encrypt.py批量加密

自动生成运行结果，注意需要check decrypt脚本能否正常运行

## 题目部署方法

### 题目运行环境

python2

### 题目部署详细过程

WHAT.zip附件直接部署到服务器中作为附件下载

### 其他说明

无

## 关键技术及解题文档

### 关键技术

了解位运算

知道Hill密码加密的根本原理

知道模运算和与运算的关系

能够编写Hill密码破解的脚本

### 解题思路

第一步：提取WHAT.zip

第二步：得到加密算法，分析得到其算法流程

第三步：通过位运算操作还原其内部核心操作其实是Hill的加密算法

第四步：编写扩展矩阵的行列变换得到flag

### 解题步骤

1、提取WHAT.zip

2、分析encrypt.py

分析其内部的原理，得到其内部的工作原理其实是Hill加密。

3、行列变换

编写行列变换得到flag

### 竞赛结果提交

LANCET{Do\_You\_Know\_Hills\_Secret}

附件

## 附件1：题目部署相关

详见题目部署附件文件夹

## 附件2：题目解题相关

详见题目解答附件文件夹

## 附件3：题目虚拟机

无

附件

## 附件1：服务检测脚本

无

## 附件2：题目部署脚本

无