|  |
| --- |
| **Github（或者Coding）账号：https://github.com/eric-huyl** |
| **个人博客关于密码学实验的链接：crypto repo的GitHub pages，待建** |
| **实验题目（中文）：密码学实验二** |
| **实验摘要（中文）：**  关于密码学实验的说明   1. 密码学实验将进行四次，每次实验，需按要求上传提交代码截图、相关结果等。 2. 请建立自己的技术博客或者其它记录载体，简单记录每次实验内容，所遇到的问题以及心得（建议）。 3. 因学校要求提交实验报告以给出成绩，我们只交一次纸质版实验报告，内容4次实验任选。 4. 最终提交时间11月30日晚23:00前。 5. 请建立自己的代码托管账号，Github或Coding或其他托管平台均可，建立合理的文件目录托管代码，请清晰命名，给出必要注释； 6. 电子版提交学在西电，提交pdf版附件命名“姓名\_学号\_密码学实验”。   实现块密码以及CBC，ECB模式相关的设计实现。 |
| **题目描述（清楚描述题目中文，写出自己的理解，请勿复制原题目）**   * + - 1. **MTC3 AES key**   **找到密钥并解密一段AES加密的密文。密钥以特定格式储存在护照的一段可读区，但是可读区缺失了一个数字。**   * + - 1. **Cryptopals Set 2**  1. **实现一个PKCS#7填充** 2. **实现CBC模式加密，用异或作为连接的函数** 3. **检测一段密文是用CBC还是ECB加密的** 4. **尝试解密一段ECB加密的文本：扮演一个攻击者，可以向明文附加一个串，然后让oracle程序使用固定的密钥加密** 5. **程序会加密一段格式化的用户信息，另一个程序解密并反序列化这段信息：扮演一个攻击者，可以操控输入和密文输出，尝试生成一个管理员身份的用户信息** 6. **在4的基础上，使用随机的附加字节长度，增大破解难度** 7. **检查是否是有效的PKCS#7填充** 8. **尝试伪造一个带有指定字符串的密文** |
| **过程（包括背景，原理：必要的公式，图表；步骤，如有必要画出流程图，给出主要实现步骤代码）**  **MTC3 AES key**  **首先看怎么找到缺失的一位。查阅资料可以知道是一个校验位。计算一下就能得出。然后按照资料中说的（故弄玄虚的）找到kseed的生成方法，然后再得出ka和kb，最后终于得到key，就可以解密了。**  **Cryptopals Set 2**   1. **这没啥好说的，看代码就行了** 2. **正常按照理论设计就行了** 3. **这个上一个实验好像做到了，就是检测重复的块，来确定是不是ECB。** 4. **首先要得到oracle使用的块大小：逐步尝试增加串的长度来改变填充，对比密文长的变化。然后检测使用的模式，可以用3的代码，虽然我们知道用的是ECB。然后用题目给出的方法对密文进行解密。** 5. **因为不能直接生成role=admin的密文，所以可以曲线救国，先生成前半部分，然后在email里面混进admin，就可以知道admin的密文。然后在生成role=的密文，再把admin的密文粘到后面，就可以了。另外要注意的点就是每段明文都会被填充到块的大小。** 6. **太hard了，不会写， 救命啊QwQ** 7. **这个挺简单的，跟1一样生成一个，验证一下就行** 8. **也不太会写。。。** |
| **总结（完成心得与其它，主要自己碰到的问题和解决问题的方法）**  **真的很难啊。真的很难啊。真的很难啊。真的很难啊。感谢gpt，不然真的不会写代码。感谢deepl的翻译，不然查资料会累死的。** |
| **参考文献（包括参考的书籍，论文，URL等，很重要）**  [**https://github.com/Rajil1213/Cryptopals-Set-2/**](https://github.com/Rajil1213/Cryptopals-Set-2/blob/master/writeup/writeup.md)  [**https://chatgpt.com/?model=auto**](https://chatgpt.com/?model=auto) |