实验 - 密码学专题一（对称密码）

实验简介

针对AES下的分组模式和填充模式完成攻击。

基础部分

1. AES Byte Flip + Orcale (60分)

实验环境:

题目：CBC目录下的task.py

远程环境：10.12.77.33:13101

实验要求:

（1）获取part_flag

2. AES Byte Flip + Orcale (20分)

实验环境:

题目：CBC目录下的task.py

远程环境：10.12.77.33:13101

实验要求:

（1）获取full_flag

3. AES Padding Orcale (20分)

实验环境:

题目：Padding目录下的task.py

远程环境：10.12.77.33:13102

实验要求:

（1）获取flag

挑战部分（Bonus)

1.求解出ASPN的密钥（20分）

实验环境:

题目：linear目录下task_withou_key.py

实验要求:

利用线性分析获取key