1. 实验原理

CPA（Correlation Power Analysis）：相关能量攻击，主要通过分析相关性来猜测密钥。

1. 仿真测量阶段，随机选择n个明文，固定正确密钥kTrue，共测得n个仿真信号，即S盒输出对应的汉明重量：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 明文-十进制 | S盒输出-十进制 | S盒输出汉明重量 |
| 1  2  3  4  5  6  7  8  9  .  .  . | 41  35  62  4  33  44  22  46  18  .  .  . | 4  2  12  7  15  4  6  7  10  .  .  . | 1  1  2  3  4  1  2  3  2  .  .  . |

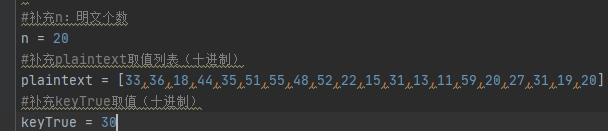
1. 攻击阶段，根据相关性进行密钥恢复。猜测所有可能的密钥，计算基于汉明重量的相关系数数组，选择相关系数数组中最大值所对应的猜测密钥即为可能密钥。两组数值和相关系数计算公式如下：



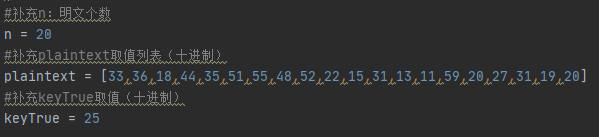
其中，，表示均值。

1. 实验代码、结果数据及数据分析
2. 完成Sboxcpa仿真-student.py程序中的空缺部分：
   1. 补充n、plaintext、keyTrue

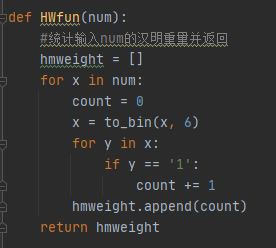
第一组：



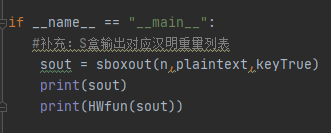
第二组：



* 1. 补充HWfun函数，返回输入的汉明重量

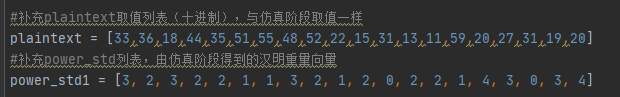
此函数本质上是计算整数转化为二进制后中1的个数，可以使用快速统计的方法。

* 1. 补充主函数，得到输出相应的汉明重量向量

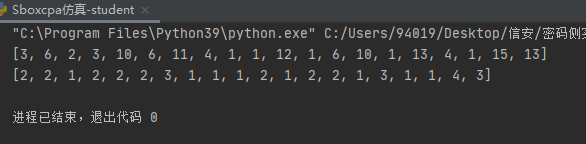


1. 完成Sboxcpa攻击-student.py程序中的空缺部分：
   1. 补充plaintext、power\_std

第一组：

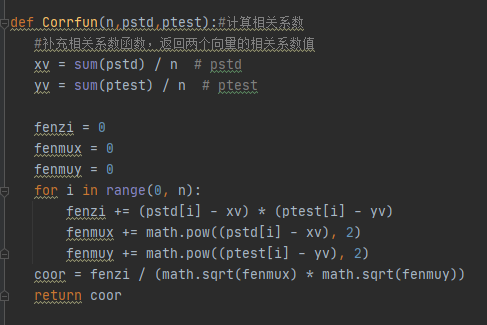


第二组：

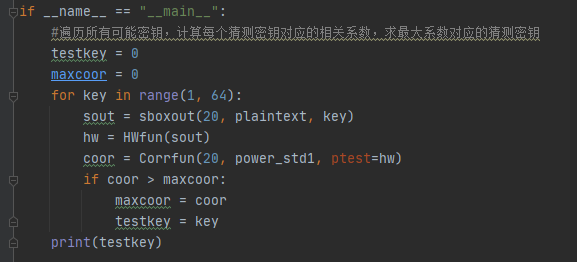


* 1. 补充相关系数Corrfun函数，返回两个向量的相关系数

根据公式推导出代码

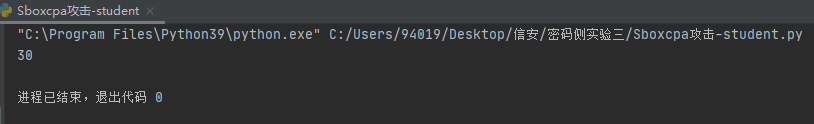


* 1. 补充主函数，求正确猜测密钥，对每个密钥计算相关系数，求出相关系数最大的猜测密钥

遍历0-63共64个密钥（密钥的所有可能性），遍历密钥得到的汉明重量数组和正确密钥得到的汉明重量数组共同带入Corrfun函数，计算相关系数，取所有相关系数中的最大值=1对应的密钥，即为正确密钥。

1. 实验数据

第一组：



第二组：

