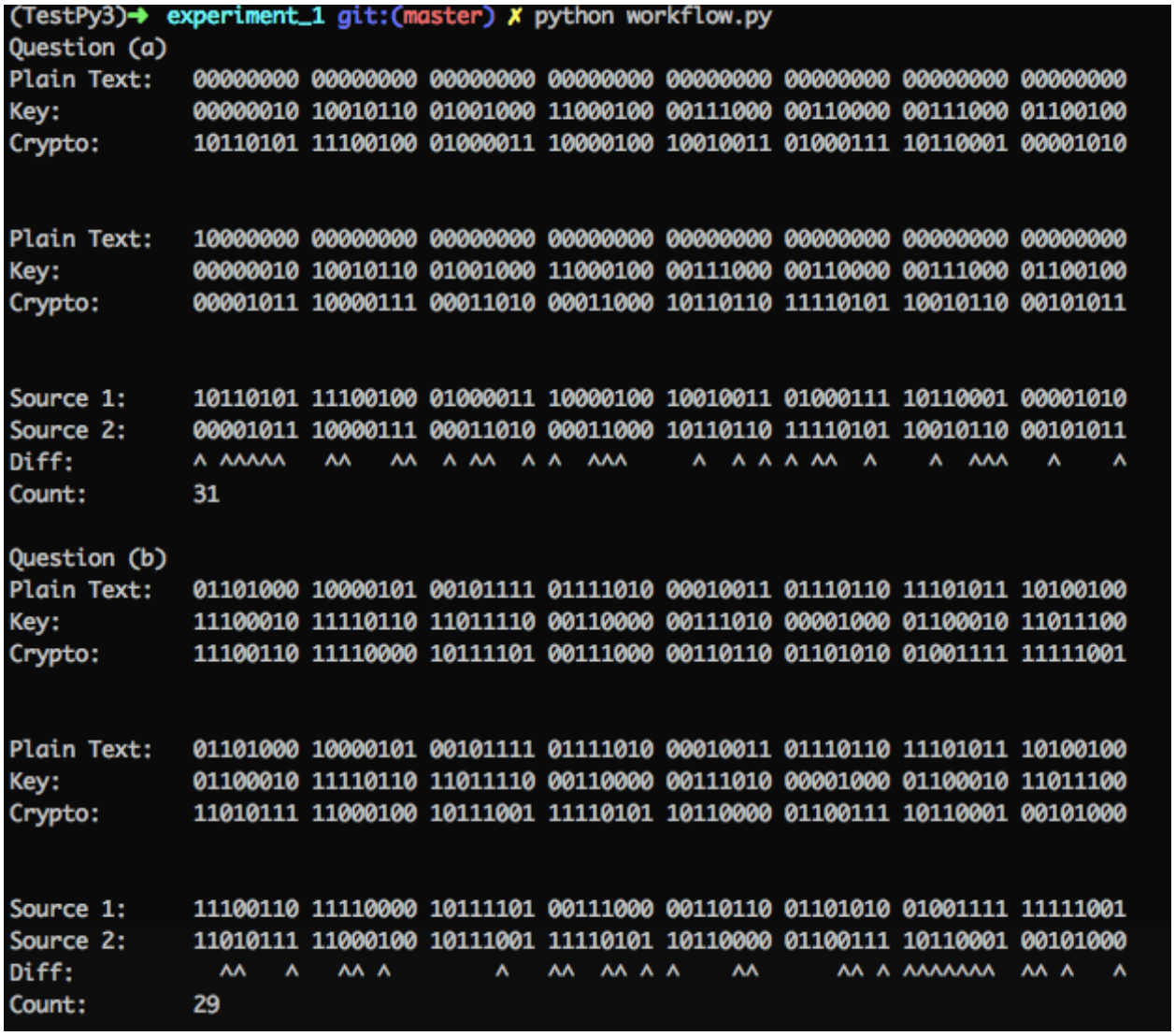
Experiment 1

实验执行结果



代码说明

代码：https://github.com/haoxun/SCUT_HomeworkOfInformationSecurity/tree/master/experiment_1

其中mydes.py是DES的Python3实现，test.py包含了三个测试用例，workflow.py包含实验报告中两个问题的求解工作流。在shell中运行”$ python workflow.py”可观测到上图输出。

什么是雪崩效应?

对于雪崩效应，Wikipedia上有如下描述：

“在密码学中，雪崩效应（Avalanche effect）指加密算法（尤其是块密码和加密散列函数）的一种理想属性。雪崩效应是指当输入发生最微小的改变（例如，反转一个二进制位）时，也会导致输出的剧变（如，输出中一半的二进制位发生反转）。在高品质的块密码中，无论密钥或明文的任何细微变化都应当引起密文的剧烈改变。该术语最早由Horst Feistel使用，尽管其概念最早可以追溯到克劳德·香农提出的扩散（diffusion）。”

在我们的实验中，Question (a)对明文的首位进行了反转操作，Question (b)对密钥的首位进行了反转操作，前者导致密文变化了31位，后者导致密文变化了29位，猜测DES具备该良好性质。进一步验证需要大量数据集的支持，并与若干benchmark算法进行对比，由于能力有限，我就到此为止了。