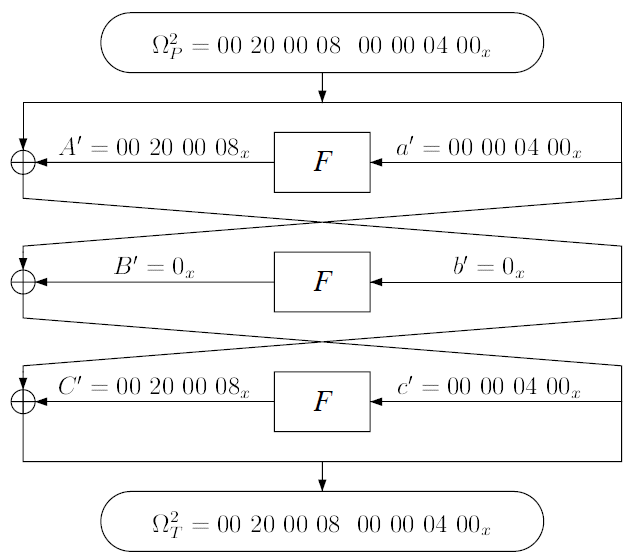
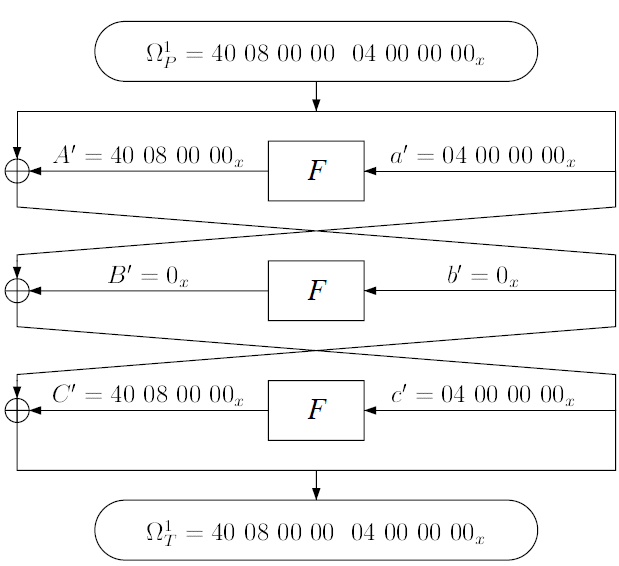
密码分析学

第2次实验：

1）仿照以下3轮DES算法（不考虑初始IP置换和最后的IP逆置换，最后一轮左右不交换）的迭代差分路线，程序搜索或手动推导其它3轮迭代差分路线（与以下示例不同的），并计算相应概率。



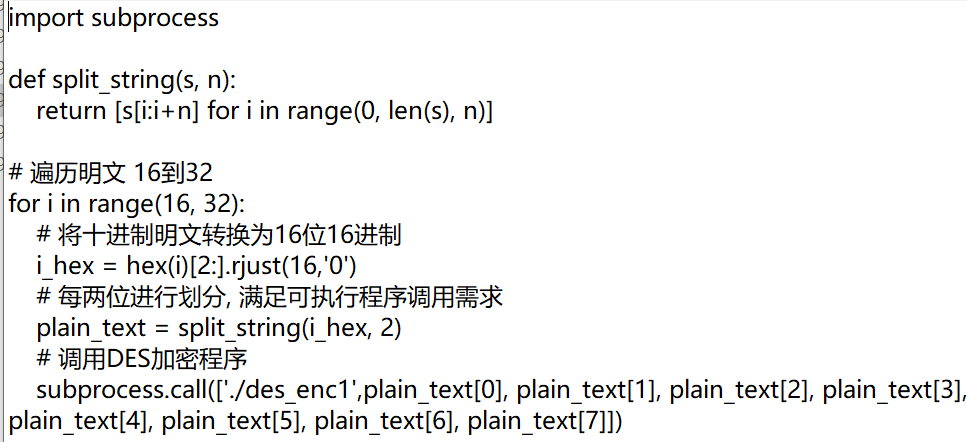
2）从1）中搜索到的路线中选取概率最大的一条（若多条概率最大，则任选其中一条即可）。设相应概率为2-*p*，随机选取10**组**不同的密钥，随机选取2-*p*+8对满足输入差分的明文对，输入**3**轮DES算法，得到相应的输出对，统计输出差分出现的频率（实测概率），与1）中概率相比较，体会差分和差分路线的含义。

可在附件des\_enc.c（6轮DES算法）代码基础上修改。

3）在1）中搜索到的路线基础上，给出6轮DES算法的密钥恢复攻击（可以仅恢复第6轮的部分轮密钥），并分析成功率和复杂度。其中，选择明文可通过调用群文件中的可执行程序来实现（1-5组用程序des\_enc1；6-10组用程序des\_enc2；11-15组用程序des\_enc3；16-20组用程序des\_enc4）。

**生成大量明文对应的密文：**

执行generate\_cipher.py程序，其中可根据需要自行指定输入的明文并调用加密程序进行加密输出密文



**注：具体细节可参考代码注释**

4）参考论文中给出的路线，尝试寻找5轮或更长轮数的迭代差分路线。

5）提交日期：2023-10-11（周三）

提交资料：实验报告+可读性较好的程序源代码

提交邮箱：3658901621@qq.com

要求同实验一。