密码分析学

第2次大作业：

1）编程实现4轮的CipherFour算法(注意最后一轮有P置换)。

2）随机选取20组不同的密钥（例如（此处数据均按16进制），某一组取值5b92, 064b, 1e03, a55f, ecbd），遍历216种16比特的输入对（x，x），输入4轮的CipherFour算法，得到相应的输出对，统计输出差分出现的频率。将选择输入对的差分改为0020，重复此实验，统计输出差分出现的频率。

3）尝试根据算法及S盒差分分布表计算差分(0,0,2,0) (0,0,2,0)的概率并与2）的实验结果进行比较。

4）利用现成的随机数生成算法，生成216对16比特的随机数（相当于随机置换的输出对），统计异或值出现的频率并与2）中结果进行比较。

5）能否找到4轮CipherFour算法的最优差分特征？最优差分呢？

6）根据压缩包中各组的数据（文件夹名即是组号，数据为固定密钥下5轮CipherFour算法的全部明密文对，plaintext\_组号.txt为所有明文，cipher\_组号.txt为所有密文，明密文按顺序对应。实际数据格式请按自己选用编程语言做适当修改。注意最后一轮无P置换），借助差分分析，实现5轮CipherFour算法的密钥恢复攻击。分别测试选择明文量100对和500对时的成功率（多次并行求解，计算求对的概率）。

7）提交日期：2020-10-17

提交资料：实验报告+可读性较好的程序源代码

提交邮箱：mimafenxixue2021@163.com

要求同作业一。