密码分析学

第1次实验：

1）给定明文wetter，按照以下给定参数，编程实现Enigma机的加密，并输出对应的密文（a从0记）。

* 接线板（5条连线）*K*1：

S = [2, 1, 0, 4, 3, 5, 7, 6, 8, 9, 24, 11, 20, 13, 14, 15, 16, 17,18, 19, 12, 21, 22, 23, 10, 25]

即a与c相连，d与e相连，g与h相连，k与y相连，m与u相连

* 扰频器组合（2个转子，无需从5个中选择）

快速转子QUICK = [0, 18, 24, 10, 12, 20, 8, 6, 14, 2, 11, 15, 22, 3, 25, 7, 17, 13, 1, 5, 23, 9, 16, 21, 19, 4]

即快速转子的表格中左侧一列为0，1，2，…，25，右侧一列0，18，24，…，4；下同

中速转子MID = [0, 10, 4, 2, 8, 1, 18, 20, 22, 19, 13, 6, 17, 5, 9, 3, 24, 14, 12, 25, 21, 11, 7, 16, 15, 23]

各转子起始点*K*2：(4, 4)

* 反射器

T = [10, 20, 14, 8, 25, 15, 16, 21, 3, 18, 0, 23, 13, 12, 2, 5, 6, 19, 9, 17, 1, 7, 24, 11, 22, 4]

即a与k相连，b与u相连，……

2）给定如下明密文数据流，1）中的两个转子和反射器的定义不变，尝试恢复密钥。（结果可能不唯一也可能无解）

明文：… wetter…

密文：…betrwpeer…

3）如果直接用穷举攻击猜测全部密钥，请理论分析需要猜测多少密钥？假设在个人电脑上每秒可进行106次加密运算，则仅用一台个人电脑大约多久可恢复出候选密钥的集合？对题目1）中实现的加密算法进行1000次加密，统计每秒可进行的加密次数，判断在个人电脑上直接进行穷举攻击是否可行？若可行，请测试并与题目2）中求解出的密钥集合进行比较。

4）选做：是否有其他密钥恢复的方法？对改进Enigma的安全性有何建议？（文字描述即可，不用实现）

5）提交日期：2023-9-25

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：

按组提交，每组提交一份即可。

请在实验报告开头写明每位组员的具体分工，如有参考文献请务必在文后标注并在正文中注明引用。各组独立完成，如果参考过其他组的文档或代码或者把自己组的进行过分享，也请在文档开头说明，避免不必要的麻烦。

提交作业时请将所有文件打包并按照 第x次作业-第x小组 命名（例如 第1次作业-第1组.zip）

其余未尽事宜参考“密码学引论“作业要求。