

密码学导论大作业

提交时间：2023 年 6 月 16 日 23: 59 之前

提交内容：大作业一和大作业二的程序，三个大作业的报告

提交格式：所有的内容打包为压缩包，压缩包的文件名为学号+姓名+密码学导论大作业，如：PB00000000_xx_密码学导论大作业

提交方式：请同学们按作业分组提交到对应的助教的邮箱中，已经交过的同学如果需要重新提交，可以在邮件中说明一下重新提交。

助教邮箱：

第一组：童蒙助教，邮箱：tm1516081@mail.ustc.edu.cn

第二组：徐昌宏助教，邮箱：xuchangh@mail.ustc.edu.cn

第三组：曹仁龙助教，邮箱：cao2000@mail.ustc.edu.cn

大作业一：

课程实践


103 / 99

题目1：单表代换统计分析工具

- 编写一个软件，辅助进行单表代换密文的破译工作。并完成本章作业1以及下文的破译工作。

```
hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf,
wxsxz qqv zqhhnf ol ozn glco zlfnc hnlhrn; nsoznj jnrqosdnc
lj fnqj kjsnfb, wxsxz sc xnjoqsfrv gljn efeceqr. zn rsdnb
qrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hfnnojcnb.
q csfyrn blgncosx cekksxb ol cnjdn zsg. zn pjnqmkgqcnb qfb
bsfnb qo ozn xrep, qo zlejc gqozngqosxqrrv ksanb, sf ozn cqgn
jllg, qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj
gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb wnfo zign
qo naqxorv gsbfsyzo, lfrv ol jnosjn qo lfxn ol pnb. zn fndnj
ecnb ozn xlcx xzqgnjc wxsxz ozn jnkljg hjldsbnc klj soc
kqdlejnb gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-klej
sf cqdsrrn jlw, nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.
```

- 该工具应当可以根据一般英文的统计分布规律给出破译建议
- 应当能够根据上下文给出破译建议（包括字母连接、字典等）
- 允许使用者设置密钥字
- 界面友好、直观、易用；语言工具不限。



1. 报告结构完整美观，重点突出，详略得当，可读性强（2分）
2. 报告内容要求有算法、实现过程、实验测试、结果分析等部分，最好能说明实验亮点，遇到问题，解决方案（6分）
3. 测试样例丰富，结果分析清晰详细（2分）
4. 抄袭0分，如有和同学，助教或老师讨论部分，请在致谢中详细说明。

大作业二:

课程实践

104 / 99

题目2: 置乱的阶的分析

- 任意置乱的阶, 就是进行不相交循环分解后各个循环长度的最小公倍数

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 7 & 6 & 1 \end{pmatrix} = \underbrace{(1, 4, 5, 7)}_{\text{阶为4}} (2, 3) (6)$$

不动点

- 问题1, 编写一个程序, 对于N个数的置乱:
 - 求最大阶T. 它意味着密文连续再加密T-1次就会恢复成明文
 - 绘制p(K)曲线。p(K)是任意一个置乱, 其阶小于K的概率
 - 你的程序能处理的N越大越好



课程实践

105 / 99

题目2: 置乱的阶的分析

- n个元素任意置乱的最大阶的计算
 - 1个n循环→阶n
 - 1个n-1循环→阶n-1
 - 1个n-2循环, 1个2循环→阶2(n-2) 或n-2
 - ...
 - 将n分解成若干数字的和, 这些数字的最小公倍数的最大值, 就是最大阶

n个元素: 最大阶 [对应的循环分解]

5:6 [3 2]

6:6 [6]

7:12 [4 3]

8:15 [5 3]

9:20 [5 4]

10:30 [5 3 2]

20:420 [7 5 4 3 1*1]

30:4620 [11 7 5 4 3]

40:27720 [11 9 8 7 5]

50:180180 [13 11 9 7 5 4 1*1]

60:1021020 [17 13 11 7 5 4 3]

70:6126120 [17 13 11 9 8 7 5]

80:19399380 [19 17 13 11 7 5 4 3 1*1]

90:116396280 [19 17 13 11 9 8 7 5 1*1]

100:232792560 [19 17 16 13 11 9 7 5 3*1]

Process returned 0 (0x0) execution time : 118.714 s

Press any key to continue.



题目2：置乱的阶的分析

- 任意置乱的阶，就是进行不相交循环分解后各个循环长度的最小公倍数

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 7 & 6 & 1 \end{pmatrix} = (1, 4, 5, 7)(2, 3)(6)$$

阶为4

不动点

- 问题2，以下是使用Logistic混沌映射构造置乱的一种常用方法：
 - 映射函数为 $x_{n+1} = \mu x_n(1 - x_n)$ ($0 < x < 1$)，当 $3.57 < \mu < 4$ 时，呈现混沌特性
 - 选定参数 μ ，任选初始值 x_0 ，迭代计算 $x_1 \sim x_N$ 。将这 N 个数排序，以每个数的位置为置乱索引。例如，若 x_i 被排在第 j 位，则置乱中将第 i 个数移至第 j 位
 - 编写一个程序，评测用该方法得到的置乱
 - 约定混沌函数的计算使用64位计算机，double类型
 - 自行考虑评测中所需要考虑的其它参数

- 报告结构完整美观，重点突出，详略得当，可读性强（2分）
- 报告内容要求有算法、实现过程、实验测试、结果分析等部分，最好能说明实验亮点，遇到问题，解决方案（6分）
- 完成题目要求，结果分析清晰详细（2分）
- 抄袭0分，如有和同学，助教或老师讨论部分，请在致谢中详细说明。

大作业三：

请从2020年-2023年的欧密会（EUROCRYPT）、美密会（CRYPTO）、亚密会（ASIACRYPT）和密码学杂志（Journal of Cryptology）自选2篇论文阅读，并完成论文报告（至少2页、Word文件、小四号字体）。每篇论文的报告至少1页，包含如下内容：

- 该论文是关于什么问题的？
- 这个问题的来龙去脉、历史发展是怎样的？
- 该论文使用什么方法，得到了什么样的结果？
- 该论文的不足之处在哪里？

- 报告结构完整美观，重点突出，详略得当，可读性强，完成基本的篇幅要求（2分）
- 说明问题背景，相关工作（1分）
- 说明论文提出的方法思想（2分）
- 阐述论文得到的结果结论（2分）
- 提出自己发现的论文的亮点（自己阅读时候有茅塞顿开，有趣的地方）（1分）
- 自己对该论文的评价，指出论文的不足（如果自己去读，会怎么做，可以天马行空，不要求实际性）（2分）
- 抄袭0分，如有和同学，助教或老师讨论部分，请在致谢中详细说明。