《密码学》课程设计实验报告

实验序号：01　　实验项目名称：古典密码

学　　号		姓　　名		专业、班	18信安3-4班
实验地点	网安基地新珈楼C203	指导教师	王张宜	时间	2020.11.24

一、　实验目的及要求

实验目的：

(1) 掌握信息安全和密码学的基本概念；

(2) 掌握密码技术的基本思想；

(3) 熟悉密码体制的组成及其分类；

(4) 熟悉置换、代替和代数等基本古典密码的编码方法；

(5) 掌握密码安全性的概念。

实验要求：

(1) 掌握古典密码设计中使用的置换、代替、XOR、迭代等技术；

(2) 理解穷举攻击、统计分析攻击与密钥空间、明文格式等方面的联系；

(3) 总结几种常见的对合算法，以及给软硬件实现带来的便利；

(4) 掌握置换、代替、XOR 等算法的编程实现与优化。

二、实验设备（环境）及要求

Windows 操作系统，高级语言开发环境

三、实验内容与步骤

1、　置换密码的实现**(必选一题)**

（1） 实现教材 p32 页第一个例子，即把明文中的字母顺序倒过来，然后截成固定长度的字母组作为密文。

提示：实现方法举例（注意字符串结束符的处理）

输入明文为数组 M[i], i∈[1,n]

输出密文为数组 C[i], i∈[1,n]

加密过程的伪码：for i=1 to n

C[i]=M[n-i+1]

解密过程的伪码：for i=1 to n

M[i]=C[n-i+1]

思考：上述运算是对合运算吗？即加解密是否可以共用一段代码实现？

（2） 实现教材 p32 页第二个例子，即把明文按某一顺序排成 m 行 n 列矩阵，其中不足部分用 Φ 填充，而 Φ 是明文中不会出现的一个符号。然后按另一顺序选出矩阵中的字母以形成密文，最后截成固定长度的字母组作为密文。

提示：实现方法举例（注意二维数组长度）

输入明文为数组 M[i] [j], i∈[1,m],j∈[1,n]

输出密文为数组 C[i] [j], i∈[1,n],j∈[1,m]

加密过程的伪码：for i=1 to m

for j=1 to n

C[j] [i]=M [i] [j]

解密过程的伪码：？

思考：上述运算是对合运算吗？即加解密是否可以共用一段代码实现？（在什么条件下是对合运算？）

2、 代替密码的实现**(必选一题)**

（1） 实现教材 p33 页加法密码

提示：实现方法举例

加密：c=((m-'A')+k)%26)+'A';

解密：m=((c-'A')-k+26)%26)+'A';

（2） 实现教材 p33 页乘法密码

思考：乘法密码中的密钥 k 的取值范围如何界定？

（3） 实现教材 p34 页仿射密码

思考：乘法密码中的密钥 k 的取值范围如何界定？共有多少种密钥可供选择？

（4） 实现教材 p35 页维吉尼亚密码

3、 代数密码的实现**(必选)**

（1） 实现教材 p40 页沃南密码

思考：上述运算是对合运算吗？即加解密是否可以共用一段代码实现？

4、 古典密码的分析

（1） 已知使用加法密码（凯撒密码的推广）加密后的密文是附表中所列，编程实现该密码算法的穷举攻击，并恢复明文和密钥。**(必选)**

（2） （选作）已知使用单表代替密码加密后的密文是

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

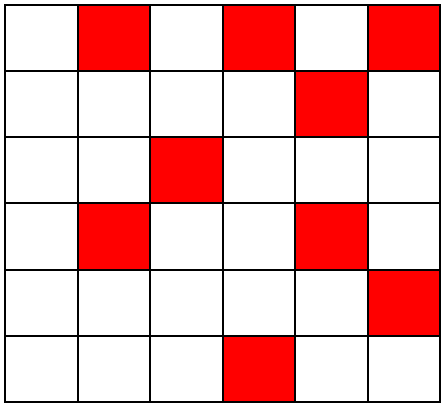
采用统计分析攻击的方法，试恢复出明文。

提示：首先统计字母频率，如高频率单字母如 z，p，t 等；再考察双字母组

合 zw 等，参考教材 p44 页的方法。

5、（选作）小手工制作：课后使用硬纸板和小刀，制作下图的旋转漏格板。

首先在硬纸板上绘制 6*6 个小正方格，并将下图中红色部分的格子割去，然后透过漏格板上的空格写字，写满后顺时针或逆时针转动漏格板，再依次书写。



思考：该方案属于置换密码，明文和密文占 36 格，密钥（漏格）占 9 格。请问有其它的密钥（漏格）排列方法吗？试给出密钥（漏格）排列方法的算法。

四、实验结果与数据处理

五、分析与讨论

六、教师评语

签名：

日期：

成绩

姓名	密文	明文	密钥
2017301510027 李兆恒	eztv kf dvvk pfl		
2016301500207 肖亦晓	ocz hvfdib ja v ivodji		
2016301500241 杨燏锂	pbb vlr xolrka		
2017301500191 吴润泽	gcvrjv krbv triv		
2017301500330 陈 磊	iccn gl rmsaf		
2018302060248 张培铭	vxkzze muuj		
2018302070001 沈思源	itrs zr trtzk		
2018302070131 谌金垚	hdggn x ctktg idas ndj		
2018302080167 王智超	ozz w kobh hc gom		
2018302110381 李江旭	qm dyp yuyw		
2018302180056 鲁震豪	ume zil chzilguncih		
2018302180057 王晨旭	qttyjyedqb ydvehcqjyed		
2018302180059 梅润元	jurer ner lbh sebz		
2018302180060 吴逸豪	kvoh rc mci rc		
2018302180062 翁 斌	qb lbh cynl nal fcbegf		
2018302180063 袁浩天	st uwtgqjr		
2018302180064 张展鹏	vod wo coo		
2018302180068 陈亚楠	j uxc xo vxernb		
2018302180069 郭点点	adkhdud ld		
2018302180070 程昊天	xahq kagd xurq		
2018302180073 郭梦卓	lmjf jayzl sl lzw kwugfv dayzl		
2018302180077 郑津哲	yssd ucwbu ghfowuvh tcf hvfss pzcqyg		
2018302180079 王怡静	ziffiq nby mcahm		
2018302180083 王丹君	wlimm nby mnlyyn		
2018302180084 倪迩畅	vd pgdjcs iwt rdgctg dc iwt gxvwi		
2018302180085 张思远	xlero csy zivc qygl		
2018302180086 严诚逸	uhapvuhs spiyhyf		
2018302180087 李宁馨	zber vasbezngvba		
2018302180088 周渴一	spzalu av aol zavyf		
2018302180091 盛威龙	wxvw hrwdda raphhbpit		
2018302180097 易子嘉	jgtgle ugrfmsr wmsp qkgjc		
2018302180098 陈映江	yu lgx cge		
2018302180099 郭瑞华	vq ngctp vq qhhgt jgnr		
2018302180151 邱振芳	hmenqlzshnm rdbtqhsx		
2018302180154 许 可	eqorwvgt uekgpeg		

2018302180160 唐炜钦	xvibo vojwfstjuz		
2018302180163 李金峰	lgac rm kccr wms		
2018302180166 梅荣新	wkh pdnlqj ri d qdwlrq		
2018302180168 徐搏鸿	nzz tjp vmjpiy		
2018302180169 叶嘉昕	kgzvnz ovfz xvmz		
2018302180174 汪 毓	smmx qv bwckp		
2018302180176 蔡文颂	givkkp xffu		
2018302180179 陈思涵	cnlm tl nlnte		
2018302180181 潘昱霏	zvyyf p ulcly avsk fvb		
2018302180183 曾一帆	rcc z nrek kf jrp		
2018302180184 林玉龙	dz qlc lhlj		
	zuoq fa yqqf kag		
	qeb jxhfkd lc x kxqflk		
	amm gwc izwcvl		
	fbuqiu jqau sqhu		
	rllw pu avbjo		
	dfshhm uccr		
	epno vn pnpvg		
	uqtta k pgxgt vqnf aqw		
	grr o cgtz zu yge		
	qm dyp yuyw		
	cum hqt kphqtocvkqp		
	zuoq fa yqqf kag		
	qeb jxhfkd lc x kxqflk		
	amm gwc izwcvl		
	fbuqiu jqau sqhu		
	rllw pu avbjo		
	dfshhm uccr		
	epno vn pnpvg		
	uqtta k pgxgt vqnf aqw		
	grr o cgtz zu yge		
	qm dyp yuyw		
例题 1:	cum hqt kphqtocvkqp	ask for information	2
例题 2:	zuoq fa yqqf kag	nice to meet you	12
例题 3:	qeb jxhfkd lc x kxqflk	the making of a nation	23