古典密码

古典密码是现在密码中体制的重要组成部分，古典密码和近代密码学发展的重要阶段，是现在密码学产生和发展的祖先吧。
虽然她现在比较简单，容易破解，但是了解它的设计原理还是非常重要的

古典密码体制的核心思想就是置换和替换。
所谓的代替就是讲铭文中的每一个子换成另外一个字符，比如说莫斯代码也差不多一样
置换就是重新排列密文，而不改变本身的意思。

α \ β	1	2	3	4	5
1	q	w	e	r	t
2	y	u	i/j	o	p
3	a	s	d	f	g
4	h	k	l	z	x
5	c	v	b	n	m

棋盘密码
棋盘密码就是讲26个英文字母加密成一个阿拉伯数字，讲26个英文字母放置在一个5x5的方程中i和j放入在一个地方中

在确定一个后，每个字母对应一个数a&，a为列号，&为行号
棋盘密码就是秘钥在一个5x5的棋盘中的字母排列情况

比如KLSQ的 明文加密成密文为 24 34 23 11.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

移位密码
设英文字符与Z26中元素之间的对应关系如下表：

加密方式
假设明文为KLSQ key=7
将明映射到z26，得出整数序列为 10 11 18 16
将数字结果加上key=7 再加上Mod 26运算 得到序列为：17 18 25 23 然后将结果转换为密文为 RSZQ

解密方式
将RSZQ密文根据对应字母进行转换，然后将结果-7并模26运算，得出结果在找到对应结果则找出明文

A	B	C	D	E	F	G	H	I	J	K	L	M
q	w	e	r	t	y	u	i	o	p	a	s	d
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
f	g	h	j	k	l	z	x	c	v	b	n	m

代换密码
直接定义置换表格π如下：

比如名为为KLSQ，得其密文为aslj

仿射密码
放射密码是一种替换密码，他的明文和密文是一一对应的密码
加密函数是 Ekey(x)=(k_1x+k_2)mod 26
解密函数是 Dkey(y)=$k_1^{-1}(y-k_2)$mod 26

其中:
-k_1^{-1}在Z26中的乘法逆元，即（k_1k^1）mod 26 = 1
-k_1为26互质
-k_2为随机数

给定英文的字符数值

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

假设需要加密的字符是KLSQ
先转换为数字组为 10 11 18 16
k_1 的所有可能值为：1,3,5,7,9,11,15,17,19,21,23，与25
在这里k_1=7，k_2=10

加密过程:
使用加密函数对明文进行加密：10 11 18 16

算式：C=Ek(m)=(k1m+k2) modn
(7 × 10 + 10) Mod 26 = 2 Mod 26 = 2
(7 × 11 + 10) Mod 26 = 9 Mod 26 = 9
(7 × 18 + 10) Mod 26 = 6 Mod 26 = 6
(7 × 16 + 10) Mod 26 = 18 Mod 26 = 18

得到密文序列为：02 09 06 18
对应字母序列：B J G S

解密过程
首先，密文序列是 2 9 6 18 对应字母为B J G S 其秘钥为7,10。