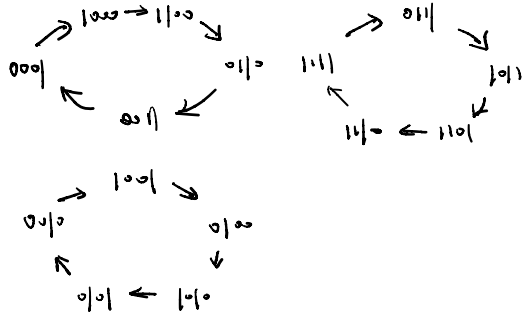
姓名：付政烨 学号：2113203 专业：信安法

1.18 考虑下列定义在 $\mathbb{Z}_2$ 上的四级线性递归序列

$$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2$$

$i \geqslant 0$。对其 16 种可能的初始向量 $(z_0, z_1, z_2, z_3) \in (\mathbb{Z}_2)^4$，分别求出其生成的密钥流的周期。

Current state	Next state
$[x_3, x_2, x_1, x_0]$	$[x_3, x_2, x_1, x_0]$
0000	0000
0001	1000
0010	1001
0011	0001
0100	1010
0101	0010
0110	0011
0111	1011
1000	1100
1001	0100
1010	0101
1011	1101
1100	0110
1101	1110
1110	1111
1111	0111



添加流序列周期为 5.

添加流序列周期为 1.

1.21 以下给出的四段密文，第一个是由代换密码加密而成，第二个是由维吉尼亚密码加密而成，第三个是由仿射密码加密而成，最后一个不知其具体的密码体制，试从密文确定明文。要求给出清晰的分析过程，包括统计分析和你进行的计算。

(b) 维吉尼亚密码

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST
```

由重合数重合法：m=1 时：$I_{c1} = 0.041$

m=2 时：$I_{c1} = 0.063$ $I_{c2} = 0.041$

m=3 时：$I_{c1} = 0.035$ $I_{c2} = 0.048$ $I_{c3} = 0.048$

m=4 时：$I_{c1} = 0.035$ $I_{c2} = 0.043$ $I_{c3} = 0.037$ $I_{c4} = 0.049$

m=5 时：$I_{c1} = 0.042$ $I_{c2} = 0.043$ $I_{c3} = 0.033$ $I_{c4} = 0.035$ $I_{c5} = 0.043$

m=6 时：$I_{c1} = 0.035$ $I_{c2} = 0.084$ $I_{c3} = 0.048$ $I_{c4} = 0.064$ $I_{c5} = 0.043$ $I_{c6} = 0.073$

所以密钥长度为6，求Mg比较有：

Mg(2)=0.050　　Mg(17)=0.071　　Mg(24)=0.057

Mg(15)=0.066　　Mg(9)=0.036　　Mg(4)=0.070

故K=(2,17,24,15,9,4)

因此，明文为：

I learned how to calculate the amount of paper needed for a room when I was at school you multiply the square foot age of the walls by the cubic contents of the floor and ceiling combined and doublebit you then allow half the total for openings such as windows and doors then you allow the other half for matching the pattern then you double the whole thing again to give a margin of error and then you order the paper

(注：上述计算工作由于过于庞大，这里采用编程用一定思路求解，详见附件)