1.18. 根据初始向量和密钥流递推式 $z_{i+4}=(z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2$ 可列表如下：

(z_0, z_1, z_2, z_3)	密钥流	周期
0 0 0 0	0000 ……	1
0 0 0 1	0001 0001 1001 1101 0011 0001	5
0 0 1 0	0010 0100 1010 0100 1010 0010	5
0 0 1 1	0011 0001 1000 1100 0110 0011	5
0 1 0 0	0100 1010 0101 0010 1001 0100	5
0 1 0 1	0101 0010 1001 0100 1010 0101	5
0 1 1 0	0110 0011 0001 1000 1100 0110	5
0 1 1 1	0111 1011 1101 1110 1111 0111	5
1 0 0 0	1000 1100 0110 0011 0001 1000	5
1 0 0 1	1001 0100 1010 0101 0010 1001	5
1 0 1 0	1010 0101 0010 1001 0100 1010	5
1 0 1 1	1011 1101 1110 1111 0111 1011	5
1 1 0 0	1100 0110 0011 0001 1000 1100	5
1 1 0 1	1101 1110 1111 0111 1011 1101	5
1 1 1 0	1110 1111 0111 1011 1101 1110	5
1 1 1 1	1111 0111 1011 1101 1110 1111	5

故当初始密钥向量为 (0,0,0,0) 时，周期为 1，其他情况周期均为 5

1.21 (b) 首先确定密钥字的长度 m，使用重合指数法。

分别令 m=1, 2, 3 ···· ，计算 m 个子串的 I_c 值分别结果如下（$I_c = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}$）：

m=1： 0.04087

m=2： 0.03846 0.04712

m=3 0.05594 0.04810 0.04826

m=4 0.03725 0.04274 0.03758 0.04905

m=5 0.04258 0.04302 0.03256 0.03528 0.04297

m=6 0.06266 0.08377 0.04935 0.06494 0.04286 0.07338

m=7 0.03061 0.04433 0.04344 0.04078 0.04433 0.04433 0.04078

⋮

可知 m=6 时各子串的重合指数最接近于 0.065，故密钥字长度为 6。

接下来确定每一位密钥。

由 m=6，可分割出子串 $y_1, y_2 \cdots, y_6$。对于任意子串 y_i，用 g 遍历 26 个字母，计算每个子串的 $M_g = \sum_{i=0}^{25} \frac{P_i \cdot f_{i+g}}{n'}$，取令 M_g 取最接近于 0.065 的 g 值即为 y_i 对应的

通过代码计算得到每个子串对应密钥：

y_1： k=2， $M_{g=2} = 0.06463$

y_2： k=17， $M_{g=17} = 0.07055$

y_3： k=24， $M_{g=24} = 0.05873$

y_4： k=15， $M_{g=15} = 0.06600$

y_5： k=19， $M_{g=19} = 0.05579$

y_6： k=14， $M_{g=14} = 0.07043$

即密钥为 (2, 17, 24, 15, 19, 14)

据此可解答，日出明文如下(已加上空格和标点)：

i learned how to calculate the amount of paper needed for a room when i was at school. you multiply the square footage of the walls by the cubic contents of the floor and ceiling combined and double it. 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.