1.18

初始向量	密钥流	周期
0000	0000 0000 0000...	1
0001	0001 1000 1100 0110 0011 0001...	5
0010	0010 1001 0100 1010 0101 0010...	5
0011	0011 0001 1000 1100 0110 0011...	5
0100	0100 1010 0101 0010 1001 0100...	5
0101	0101 0010 1001 0100 1010 0101...	5
0110	0110 0011 0001 1000 1100 0110...	5
0111	0111 1011 1101 1110 1111 0111...	5
1000	1000 1100 0110 0011 0001 1000...	5
1001	1001 0100 1010 0101 0010 1001...	5
1010	1010 0101 0010 1001 0100 1010...	5
1011	1011 1101 1110 1111 0111 1011...	5
1100	1100 0110 0011 0001 1000 1100...	5
1101	1101 1110 1111 0111 1011 1101...	5
1110	1110 1111 0111 1011 1101 1110...	5
1111	1111 0111 1011 1101 1110 1111...	5

由此可知，当初始向量为 0000 时，密钥流周期为 1；其余时刻密钥流周期均为 5。

1.21（b）

首先使用重合指数法可得：
m=1
0.04078352409212943
m=2
0.038461538461538464 0.046906187624750496
m=3
0.055941845764854614 0.04777992277992278 0.04826254826254826
m=4
0.03725490196078431 0.04274239816408491 0.037578886976477335
0.047905909351692484
m=5
0.04258121158911326 0.04302019315188762 0.03211216644052465
0.035278154681139755 0.04296698326549073
m=6
0.06265664160401002 0.08116883116883117 0.04935064935064935
0.06493506493506493 0.04285714285714286 0.07337662337662337

可以猜测该密文的密钥长度为 6

接下来使用 Mg 法求密钥
对于第一组，Mg(C) = 0.06463157894736843
对于第二组，Mg(R) = 0.07041071428571428
对于第三组，Mg(Y) = 0.05873214285714288
对于第四组，Mg(P) = 0.06599999999999999
对于第五组，Mg(T) = 0.055785714285714286
对于第六组，Mg(O) = 0.07042857142857142

因此密钥为 CRYPTO
最终得到的明文为：
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 double it you then allow half the total fnr 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