1. Compute the period of the linear congruential generator $X_{n+1} = 3X_n + 2 \bmod 23$ with various initial value X_0

$X_{n+1} = (aX_n + c) \bmod m \quad 0 < a < m,\ 0 \le c < m$

$X_0 = 1 \quad X_1 = (3 \cdot 1 + 2) \bmod 23 = 5,\ X_2 = (3 \cdot 5 + 2) \bmod 23 = 17,\ X_3 = (3 \cdot 17 + 2) \bmod 23 = 7,\ X_4 = 0,\ X_5 = 2,\ X_6 = 8,\ X_7 = 3,\ X_8 = 11,\ X_9 = 12,\ X_{10} = 15,\ X_{11} = 1, \ldots$

$X_0 = 2 \quad X_1 = (3 \cdot 2 + 2) \bmod 23 = 8,\ X_2 = (3 \cdot 8 + 2) \bmod 23 = 3,\ X_3 = (3 \cdot 3 + 2) \bmod 23 = 11,\ X_4 = 12,\ X_5 = 15,\ X_6 = 1,\ X_7 = 5,\ X_8 = 17,\ X_9 = 7,\ X_{10} = 0,\ X_{11} = 2, \ldots$

$X_0 = 4 \quad X_1 = 14,\ X_2 = 21,\ X_3 = 19,\ X_4 = 13,\ X_5 = 18,\ X_6 = 10,\ X_7 = 9,\ X_8 = 0,\ X_9 = 20,\ X_{10} = 16,\ X_{11} = 4, \ldots$

period = 11 with $X_0 = 22$ period = 1

2. Compute the 16 output bits of the LFSR $B_2X^2 + B_0X^4$ with initial values $B_3B_2B_1B_0 =$ 1010 and 1011. What are their periods?

state	B_3	B_2	B_1	B_0	B_0ÅB_2	output
initial 0	1	0	1	0	0	0
1	0	1	0	1	0	1
2	0	0	1	0	0	0
3	0	0	0	1	1	1
4	1	0	0	0	0	0
5	0	1	0	0	1	0
6	1	0	1	0	0	0
7	0	1	0	1	0	1
8	0	0	1	0	0	0
9	0	0	0	1	1	1
10	1	0	0	0	0	0
11	0	1	0	0	1	0
12	1	0	1	0	0	0
13	0	1	0	1	0	1
14	0	0	1	0	0	0
15	0	0	0	1	1	1

state	B_3	B_2	B_1	B_0	B_0ÅB_2	output
initial 0	1	0	1	1	1	1
1	1	1	0	1	0	1
2	0	1	1	0	1	0
3	1	0	1	1	1	1
4	1	1	0	1	0	1
5	0	1	1	0	1	0
6	1	0	1	1	1	1
7	1	1	0	1	0	1
8	0	1	1	0	1	0
9	1	0	1	1	1	1
10	1	1	0	1	0	1
11	0	1	1	0	1	0
12	1	0	1	1	1	1
13	1	1	0	1	0	1
14	0	1	1	0	1	0
15	1	0	1	1	1	1

period : 0101000101000101

period ; 1101101101101101

3. Suppose you have an entropy source that produces independent bits, where bit 1 is generated with probability 0.5+p and bit 0 is generated with probability 0.5-p, where 0<p<0.5. Consider the conditioning algorithm that examines the output bit stream as a sequence of non-overlapping pairs. Discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.

   a. What is the probability of occurrences of each pair in the original sequence?
   b. What is the distribution of occurrences of bits 0 and 1 in the modified sequence?
   c. What is the expected number of input bits in order to generate an output bit

a. probability of 00 : $(0.5-p)^2$ probability of 01 : $(0.5-p)(0.5+p)$ probability of 10 : $(0.5+p)(0.5-p)$
probability of 11 : $(0.5+p)^2$

b. Since 01 pair is replaced with 0 and 10 pair with 1, and 01 and 10 have same probability, so the distribution are
0: $0.25-p^2$ 1: $0.25-p^2$

c. Expected pairs to get one output bit : $\frac{1}{P(01)+P(10)}$ since each pair consists of 2 bits the expected number
is $\frac{2}{P(10)+P(01)} = \frac{2}{(0.5-p)(0.5+p)+(0.5-p)(0.5+p)} = \frac{1}{(0.25-p^2)}$

4. Consider the RSA encryption system. Let n = 29 × 43 = 1247 and e = 17.

   a. What is the private key d?
   b. What is the plaintext of ciphertext C=1123?

$n = 29 \times 43 = 1247$ $\phi(n) = (29-1)(43-1) = 1176$

a. $d = e^{-1} \bmod \phi(n) = 17^{-1} \bmod 1176 = 761$ $17n = 1176k+1$ $(n=761 . k=11)$

b. $M = 1123^{761} \bmod 1247 = 1104$

1176		1	0
17		0	1
3	69	1	-69
2	5	-5	346
1	1	6	-415

$1176-415 = 761$

5. Consider RSA encryption with n=136127. Assume that Alice has key pair $PU_A = (17, n)$ and $PR_A = (79553, n)$. Alice knows that Bob uses the same n to set up his key pair and $PU_B = (31, n)$. Alice intercepts a ciphertext C=3761 which is sent to Bob by Carol. Show that Alice can decrypt C without factoring n.

$k\phi(n) = 79553 \times 17 - 1 = 1352400$

$d' = 31^{-1} \bmod 1352400 = 1134271$

i	b_i	q_i	x_i	y_i
-1	1352400		1	0
0	31		0	1
1	25	43625	1	-43625
2	6	1	-1	43626
3	1	4	5	-218129

$P = C^{d'} \bmod n = 3761^{1134271} \bmod 136127 = 33745$

$k\phi(n) = e_A d_A - 1$

$d_B' = e_B^{-1} \bmod k\phi(n)$

$P = C^{d_B'} \bmod n$

$= M^{e_B d_B'} \bmod n$

$= M^{e_B (k\phi(n))} \bmod n$

$= M^{k'(k\phi(n))+1} \bmod n$

$= (M^{\phi(n)})^{k'k} \cdot M \bmod n$

$= 1^{k'k} \cdot M \bmod n$

$= M$