

1. The ciphertext printed below was encrypted using a substitution cipher. The objective is to decrypt the ciphertext without knowledge of the key.
  - a. Provide the relative frequency of all letters A...Z in the ciphertext.
  - b. Decrypt the ciphertext with help of the relative letter frequency of the English language (e.g., search Wikipedia for letter frequency analysis). Note that the text is relatively short and might not completely fulfill the given frequencies from the table.
  - c. Find the key and provide letter frequency for the given text.

Ciphertext:

CKCLBAELDK DGJ LFNSMBCA CGQEGCCAI JCUCKFS DGJ LACDBC SAFJMLBI BHDB  
 LHDGQC BHC OFAKJ DGJ NDVC FMA KEUCI CDIECA BHC LCKK SHFGCI OC JCSCGJ FG  
 BHC LFNSMBCAI MICJ EG GDBEFGDK ICLMAEBR DGJ BHC CKCLBAELDK IRIBCNI BHDB  
 NDVC FMA LDAI FSCADBC OCAC DKK LACDBCJ TR CKCLBAELDK DGJ LFNSMBCA  
 CGQEGCCAI DB OSE OC VCCS BHDB SAFQACII NFUEGQ PFAODAJ OEBH FMA  
 EGGFUDBEUC ACICDALH DGJ FMB-FP-BHC TFY DSSAFDLHCI BHC JCSDABNCGB FP  
 CKCLBAELDK DGJ LFNSMBCA CGQEGCCAEGQDB OSE LHDKKCGQCI IBMJCGBI BF  
 SMIH BHCNICKUCI BF MGJCAIBDGJ IFLECBRI DGJ BCLHGFKFQRI LFNSKCY EIIMCI EG  
 D TAFDJCA LFGBCYB BHDG OHDBI EG PAFGB FP BHCN OC ODGB FMA IBMJCGBI  
 OHCBHCA BHC DAC CDAGEGQ DG MGJCAQADJMDBC NEGFAFA D JFLBFADBC BF  
 BDLVKC IFLECBRI NFIB SACIIEGQ SAFTKCNI DGJ MGLFUCA GCO ODRI FP IFKUEGQ  
 BHCN OHCBHCA EBI JCUCKFSEGQ IRIBCNI BHDB LDG KFLDBC PEACPEQHBCAI EG  
 BHC NEJJKC FP D TMAGEGQ TMEKJEGQ FA LACDBEGQ GCMAFSAFIBHCBELI BHDB  
 KFFV DGJ PMGLBEFG KEVC GDBMADK KENTI FMA PDLMKBR DGJ IBMJCGBI DAC DB  
 BHC PAFGB CJQC FP ACNDAVDTKC EGGFUDBEFG OHEKC DJUDGLEGQ  
 BCLHGFKFQECI EI DB FMA LFAC OC DKIF BDVC HMNDG LFGGCLBEFGI UCAR  
 ICAEFMIKR EG CLC OC SAEJC FMAICKUCI FG BHC PDNEKR-KEVC DBNFISHCAC OC  
 LMKBEUDBC; PDLMKBR IBMJCGBI DGJ IBDPP CGLFMADQC CDLH FBHCAI CUCAR  
 IMLLCII DGJ DAC BHCAC PFA BHC LHDKKCGQCI TFBH EG BHC LKDIIAFFN DGJ EG  
 KEPC

2. Do the followings for the given LFSRs.
  - i.  $(m, \text{gatepositions}, \text{intialstate}) = (9, (C0, C1, \dots, C7, C8), (Z0, Z1, \dots, Z7, Z8)) = (9, (1, 0, 1, 0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 1, 0, 1, 0, 0))$
  - ii.  $(m, \text{gatepositions}, \text{intialstate}) = (9, (C0, C1, \dots, C7, C8), (Z0, Z1, \dots, Z7, Z8)) = (9, (0, 0, 1, 0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 1, 0, 1, 0, 0))$ 
    - a. Draw a circuit diagram for the given LFSR.
    - b. What is the maximum length of the key stream this LFSR can produce?
    - c. Compute the first 30 bits of the output bit stream.
    - d. Use Vernam Cipher to encrypt the following plaintext using the bit stream generated in part b. P=`111011000001101110110100111110`

# Question 1






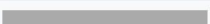
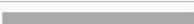
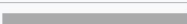
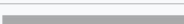
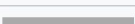
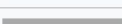















## Part A

Letter frequency of ciphertext:

Letter in ciphertext	Number of letters/Frequency
A	75
B	100
C	150
D	86
E	58
F	76
G	83
H	45
I	70
J	40
K	47
L	50
M	37
N	24
O	19
P	19
Q	23
R	15
S	24
T	9
U	15
V	9
W	0
X	0
Y	3
Z	0

## Part B

I used this reference as a starting point for decrypting the substitution cypher, which depicts the frequency of letters that appear in the English language:

Letter ↕	relative frequency in the	
	Texts ▼	
e	13%	
t	9.1%	
a	8.2%	
o	7.5%	
i	7%	
n	6.7%	
s	6.3%	
h	6.1%	
r	6%	
d	4.3%	
l	4%	
c	2.8%	
u	2.8%	
m	2.4%	
w	2.4%	
f	2.2%	
g	2%	
y	2%	
p	1.9%	
b	1.5%	
v	0.98%	
k	0.77%	
j	0.15%	
x	0.15%	
q	0.095%	
z	0.074%	

Next, I picked out words in the cipher that were easy to identify like “and” or “computer” and made changes until I had the correct letter substitutions:

Letter in ciphertext	Decrypted letter
A	R
B	T

C	E
D	A
E	I
F	O
G	N
H	H
I	S
J	D
K	L
L	C
M	U
N	M
O	W
P	F
Q	G
R	Y
S	P
T	B
U	V
V	K
W	J
X	Q
Y	X
Z	Z

Using this key, I decrypted the ciphertext:

ELECTRICAL AND COMPUTER ENGINEERS DEVELOP AND CREATE PRODUCTS THAT CHANGE THE WORLD AND MAKE OUR LIVES EASIER THE CELL PHONES WE DEPEND ON THE COMPUTERS USED IN NATIONAL SECURITY AND THE ELECTRICAL SYSTEMS THAT MAKE OUR CARS OPERATE WERE ALL CREATED BY ELECTRICAL AND COMPUTER ENGINEERS AT WPI WE KEEP THAT PROGRESS MOVING FORWARD WITH OUR INNOVATIVE RESEARCH AND OUT-OF-THE BOX APPROACHES THE DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING AT WPI CHALLENGES STUDENTS TO PUSH THEMSELVES TO UNDERSTAND SOCIETYS AND TECHNOLOGYS COMPLEX ISSUES IN A BROADER CONTEXT THAN WHATS IN FRONT OF THEM WE WANT OUR STUDENTS WHETHER THEY ARE EARNING AN UNDERGRADUATE MINOR OR A DOCTORATE TO TACKLE SOCIETYS MOST PRESSING PROBLEMS AND UNCOVER NEW

WAYS OF SOLVING THEM WHETHER ITS DEVELOPING SYSTEMS THAT CAN LOCATE FIREFIGHTERS IN THE MIDDLE OF A BURNING BUILDING OR CREATING NEUROPROSTHETICS THAT LOOK AND FUNCTION LIKE NATURAL LIMBS OUR FACULTY AND STUDENTS ARE AT THE FRONT EDGE OF REMARKABLE INNOVATION WHILE ADVANCING TECHNOLOGIES IS AT OUR CORE WE ALSO TAKE HUMAN CONNECTIONS VERY SERIOUSLY IN ECE WE PRIDE OURSELVES ON THE FAMILY-LIKE ATMOSPHERE WE CULTIVATE; FACULTY STUDENTS AND STAFF ENCOURAGE EACH OTHERS EVERY SUCCESS AND ARE THERE FOR THE CHALLENGES BOTH IN THE CLASSROOM AND IN LIFE

## Part C

The key found in part B is: rteaionhsdlcumwfgypbvkJqXZ

The letter frequency for the given text is:

Letter in ciphertext	Decrypted letter	Number of letters/Frequency
A	R	75
B	T	100
C	E	150
D	A	86
E	I	58
F	O	76
G	N	83
H	H	45
I	S	70
J	D	40
K	L	47
L	C	50
M	U	37
N	M	24
O	W	19
P	F	19
Q	G	23
R	Y	15
S	P	24

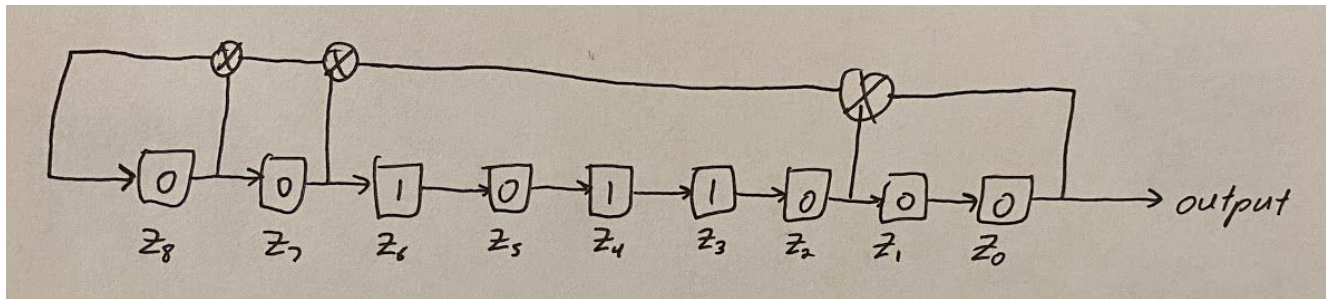
T	B	9
U	V	15
V	K	9
W	J	0
X	Q	0
Y	X	3
Z	Z	0

## Question 2

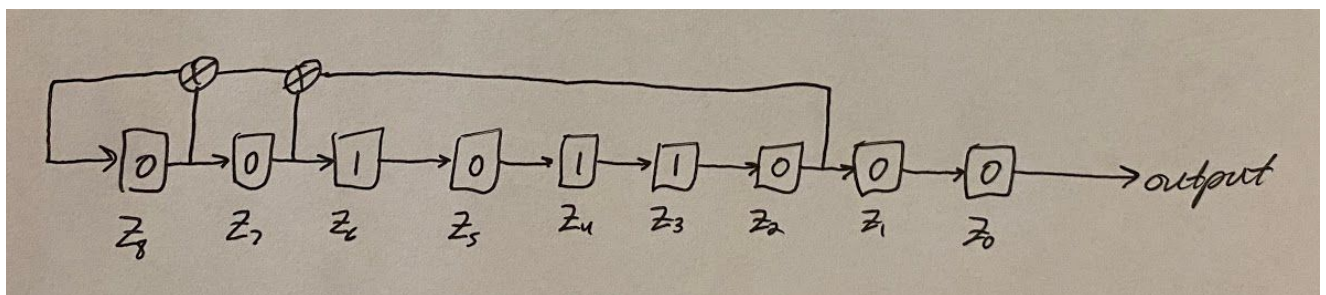
## Part A

Diagrams:

i.



ii.



calculated the max period by hand but also made a java program to check by brute force if the actual period was the same as the max period. In my findings, I concluded that the period of both LFSRs was indeed the max period of  $2^9 - 1$ , or 511. The code I made can be found here: <https://hatebin.com/rqiftjeeea>

i. Period = 511

ii. Period = 511

## Part C

i. First 30 bits: 000110100010000111000010100001

S0	0
S1	0
S2	0
S3	1
S4	1
S5	0
S6	1
S7	0
S8	0
S9	0
S10	1
S11	0
S12	0
S13	0
S14	0
S15	1
S16	1
S17	1
S18	0
S19	0
S20	0
S21	0
S22	1

S23	0
S24	1
S25	0
S26	0
S27	0
S28	0
S29	1

ii. First 30 bits: 000110100010101100011110111111

S0	0
S1	0
S2	0
S3	1
S4	1
S5	0
S6	1
S7	0
S8	0
S9	0
S10	1
S11	0
S12	1
S13	0
S14	1
S15	1
S16	0
S17	0
S18	0
S19	1
S20	1
S21	1
S22	1
S23	0



S24	1
S25	1
S26	1
S27	1
S28	1
S29	1

## Part D

To encrypt the plaintext using binary, I simply took the XOR of each bit from the key and the plaintext one by one.

i. Encrypted plaintext: 111101100011101001110110011111

ii. Encrypted plaintext: 111101100011000010101010000001

## Bonus Question

**Given: Consider an LFSR with  $m$  registers. Show that you can find gate positions if you have  $2m$  consecutive output bits.**

Given  $2m$  outputs, we can determine that the number of iterations that can be formed given those outputs will be  $m+1$ .

**For example**, if an output from LFSR of length 3 is given, there will be 6 outputs, which form 4 iterations:

Given output: 111001

Iterations:

001

100

110

111

**For example**, if an output from LFSR of length 4 is given, there will be 8 outputs, which form 5 iterations:

Given output: 10011010

Iterations:

1010

1101

0110

0011

1001

Additionally, we know that for any LFSR, the maximum number of closed gates can be equal to  $m$ . This means that for an LFSR with  $m$  bits, there are  $m$  unknowns. Given that we have  $m+1$  iterations and  $m$  unknowns, we can form a system of equations consisting of  $m$  unknowns and  $m+1$  equations, meaning it is always possible to find all the unknowns which would be the states of the gates in the LFSR.