Lab 4

1) **The following message is encrypted using the single-letter substitution code. Use frequency analysis the message to get the original plaintext.**

ODZKG FHOXP FOEYL HZEZK UXTGY OAGTA
OATAX UOAUO DDUPY DTNPU XXKGG YADRV
YAUGO HSOXT FDZXY ERYRY XTFOA PYOHU
PYWKT YUUOQ QTANZ LUPYH OTAON OTAXU
UPYVT AGZVX UPYVT AGBYN TAXUZ NKXUO
AGUPY HOTAB YFZEY XEZHY XUYOG ROAGH
OQTGT PYOHO DZKGX FHYYF PDTSY OUHYY
OHYAZ BHOAF PONOT AXUUP YVTAG ZVRYU
UPYHY UHYYX AYOHB RTNZU ZUPYL HZAUG
ZZHOA GZQYA TUQYY HTANZ KUTAU ZUPYG
OHSAY XXZLA TNPU

……

……

……

……

2) **Let the message be: APRIL SHOWERS BRING MAY FLOWERS. Let the key word be: RHYME.**

Use Vigenère cipher square to encrypt the plaintext and get the cipher message:

………

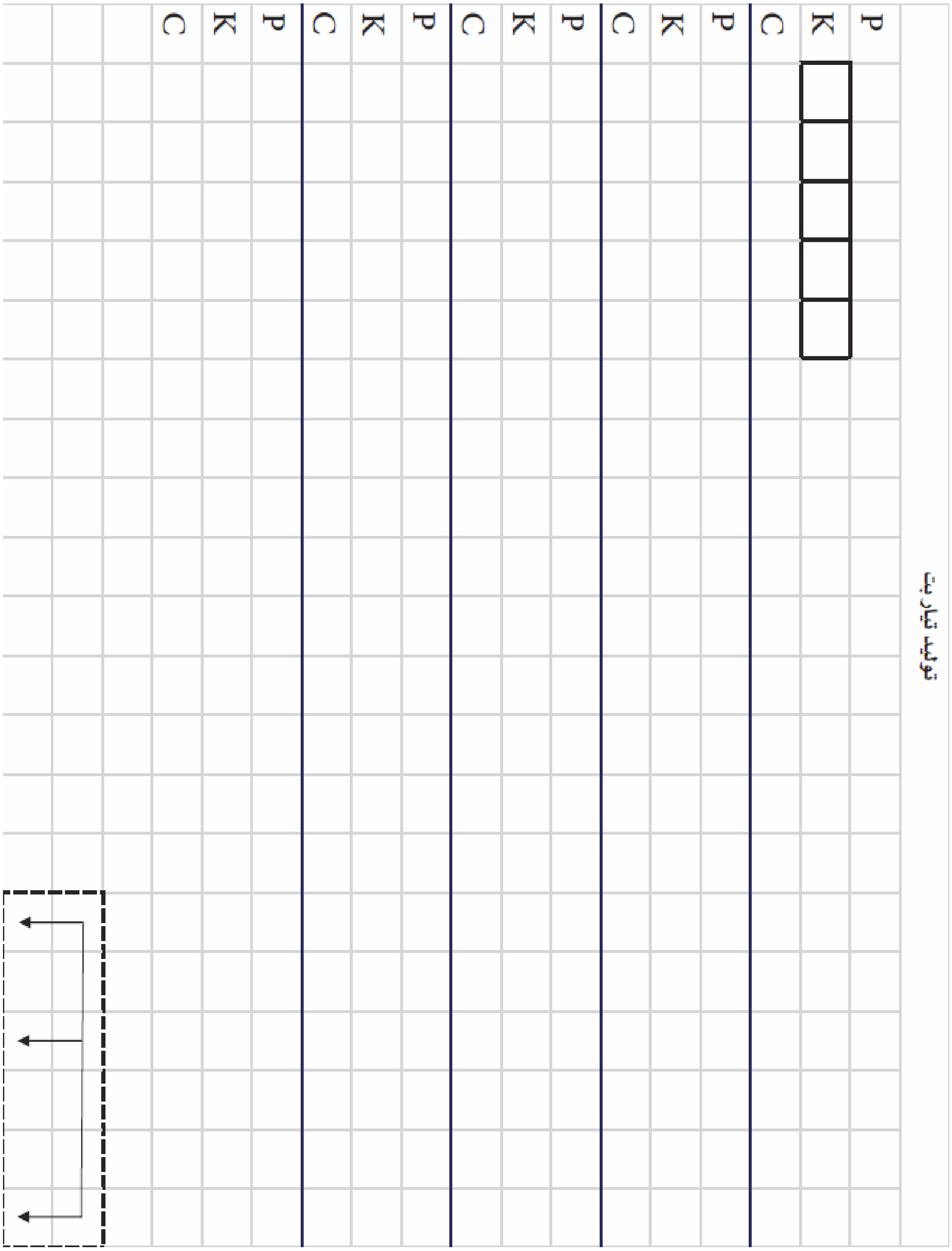
3) **Consider DES encryption method:**

   A) **Encrypt the first two characters from your first name using the first of two characters in your family name as a key.**

   B) **Decrypt the word (SLIDE) using the keyword (FIVE)**

4) Use the following chart to generate a key based on Linear Feedback Shift Registers method. Pick any seed number and use the guided locations at the left-bottom corner. Then use your key to encrypt the following message

MEET HIM AT THE HALL



a) **How long will it take your key to start repeating? If there is no repeating, it means there your answer is incorrect.**

b) **Unfortunately, All LFSRs repeat after a certain number of clock ticks. What are the possible ways to ensure secure encryption for our messages using LFSR?**

c) **What is the reason that zero seeds are not suitable for use in any LFSR?**

d) **What are the maximum period length that can be reached for ……. non-zero seed if length of the register:**

- **L = 2**
- **L = 3**
- **L = 5**
- **L = 32**

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