19CSE331 Cryptography

Assignment Questions

Do the cryptanalysis for the following cipher texts using Substitution Cipher

1.

Y I F Q F M Z R W Q F Y V E C F M D Z P C V M R R Z W N M D Z V E J B T X C D D U M J N D I

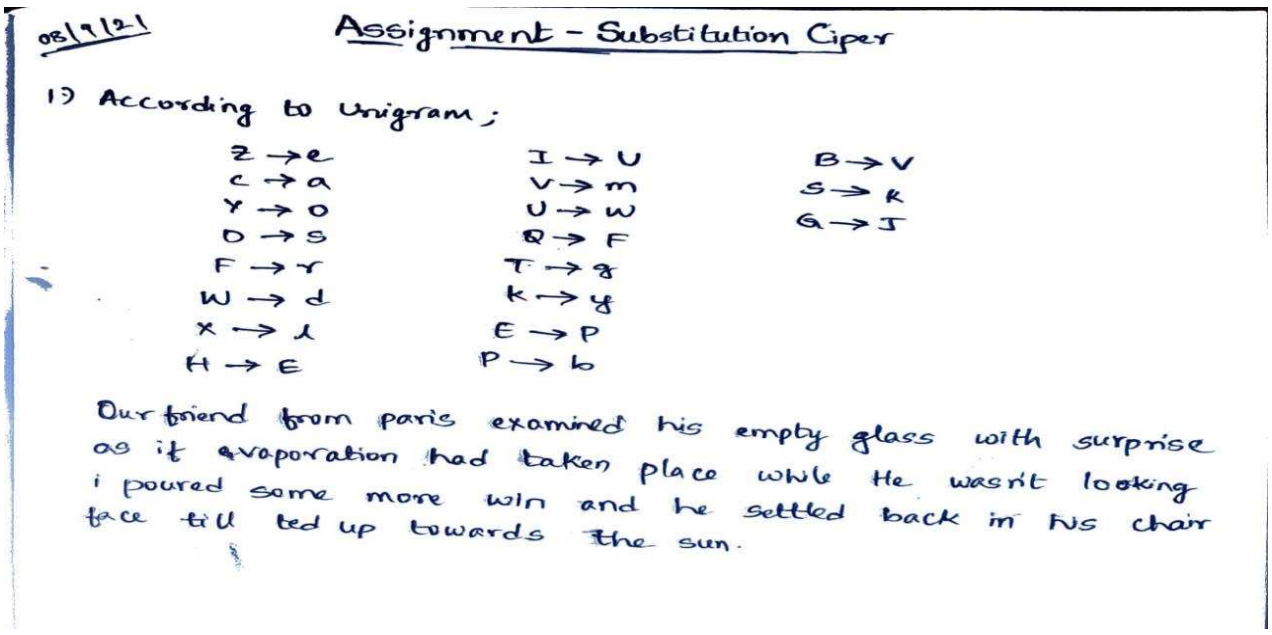
F E F M D Z C D M Q Z K C E Y F C J M Y R N C W J C S Z R E X C H Z U N X Z N Z U C D R J X

Y Y S M R T M E Y I F Z W D Y V Z V Y F Z U M R Z C R W N Z D Z J J X Z W G C H S M R N M

D H N C M F Q C H Z J M X J Z W I E J Y U C F W D J N Z D I R

Answer:

OUR FRIEND FROM PARIS EXAMINNED HIS EMPTY GLASS WITH SURPRISE AS IF EVAPORATION HAD TAKEN PLACE WHLE HE WASNT LOOKING I POURED SOMEMORE WINE AND HE SETTLED BACK IN HIS CHAIR FACE TILTED UP TOWARDS THE SUN



08/9/21

Assignment - Substitution Ciper

1) According to Unigram;

Z → e	I → U	B → V
C → a	V → m	S → K
Y → O	U → W	G → J
O → S	Q → F	
F → r	T → g	
W → d	K → y	
X → l	E → P	
H → E	P → b	

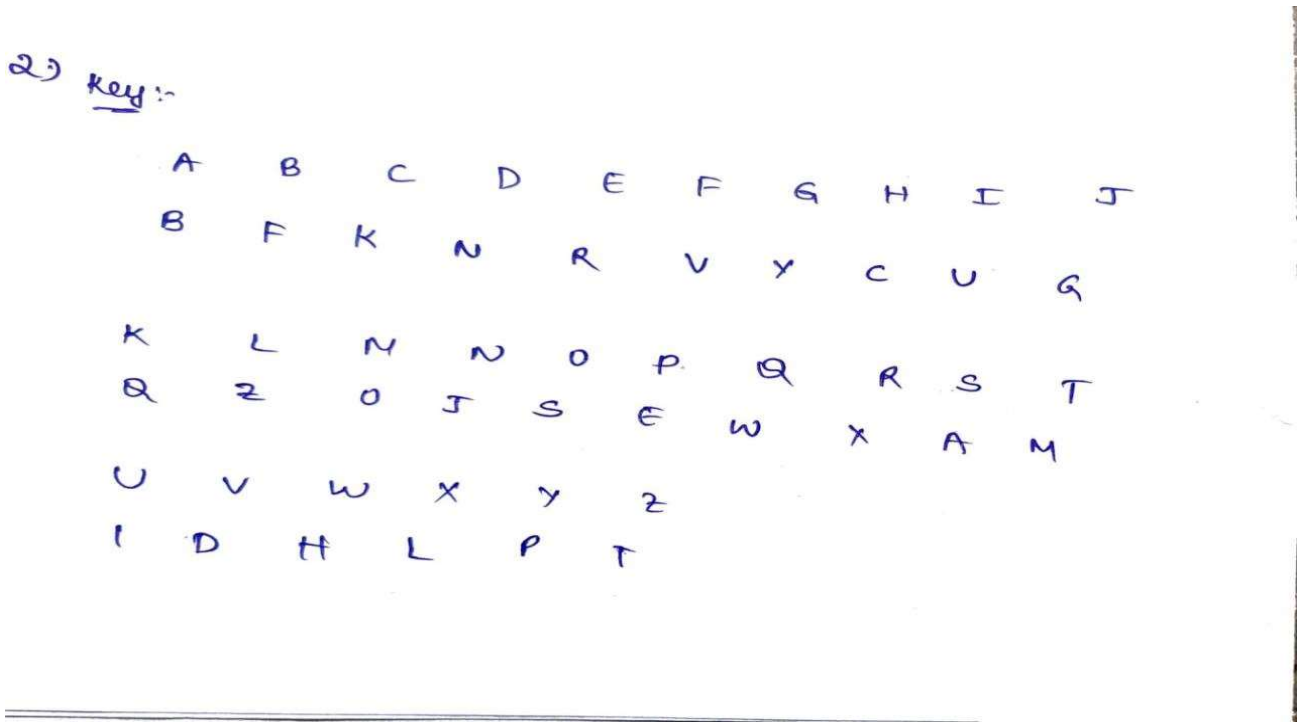
Our friend from paris examined his empty glass with surprise as if evaporation had taken place while He wasn't looking i poured some more win and he settled back in his chair face tilted up towards the sun.

2.

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

Answer :

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACT SHAVE BEEN MADE WITH POLITICAL REPRESENT AT OR SOFT VIET CONG IN MOSCOW



3.

D LJELKOKJKOUV COSIYM OL IDMRYM KU CMDCZ KIDV D CDYLDM COSIYM EJK GY CDV LKOXX JLY PMYQJYVCB DVDXBLOL KU POVR KIY WULK CUWWUV XYKKYML. O SMUWOLYR BUJ KIDK O GUJXR JLY DXX KGYVKB LOF

XYKKYML LU KIDK WYDVL KIDK O IDHY TUK KU DRR YFKMD GUMRL LJCI DL NYXXB DVR AUU.

3) Since not much alphabet letter by itself can be used alone,
D → A & I → O should be the other letter.

After initial guess :-

A → D
I → O

a LJELKiKJKiUV CiSIYM iL IaMRYM KU CMaC2 KIaV aCaYLAM CiSIYM EJK GY CaV LKiXX JLY PMYQJYVCB aVaXBLiL KU PiVR KIY WULK CUWWUV XYKKYML. i SMUWiLYR BUJ KIaK i GUIXR JLY aXX KGYVKB LiF XYKKYML LU KIaK WYaVL KIaK I IaHY TUK KU aRR YFKMa GUMRL LJCI aL NYXXB aVR AUU.

most appearing :-
K — 25
D → 20
Y → 20
L → 19
U → 15

less :- F, → 2
(Z, Q, H, I, N, A) → 1

then from AUU,
↓
3 letters with repeating letters
Eg :- too, zoo (took this)

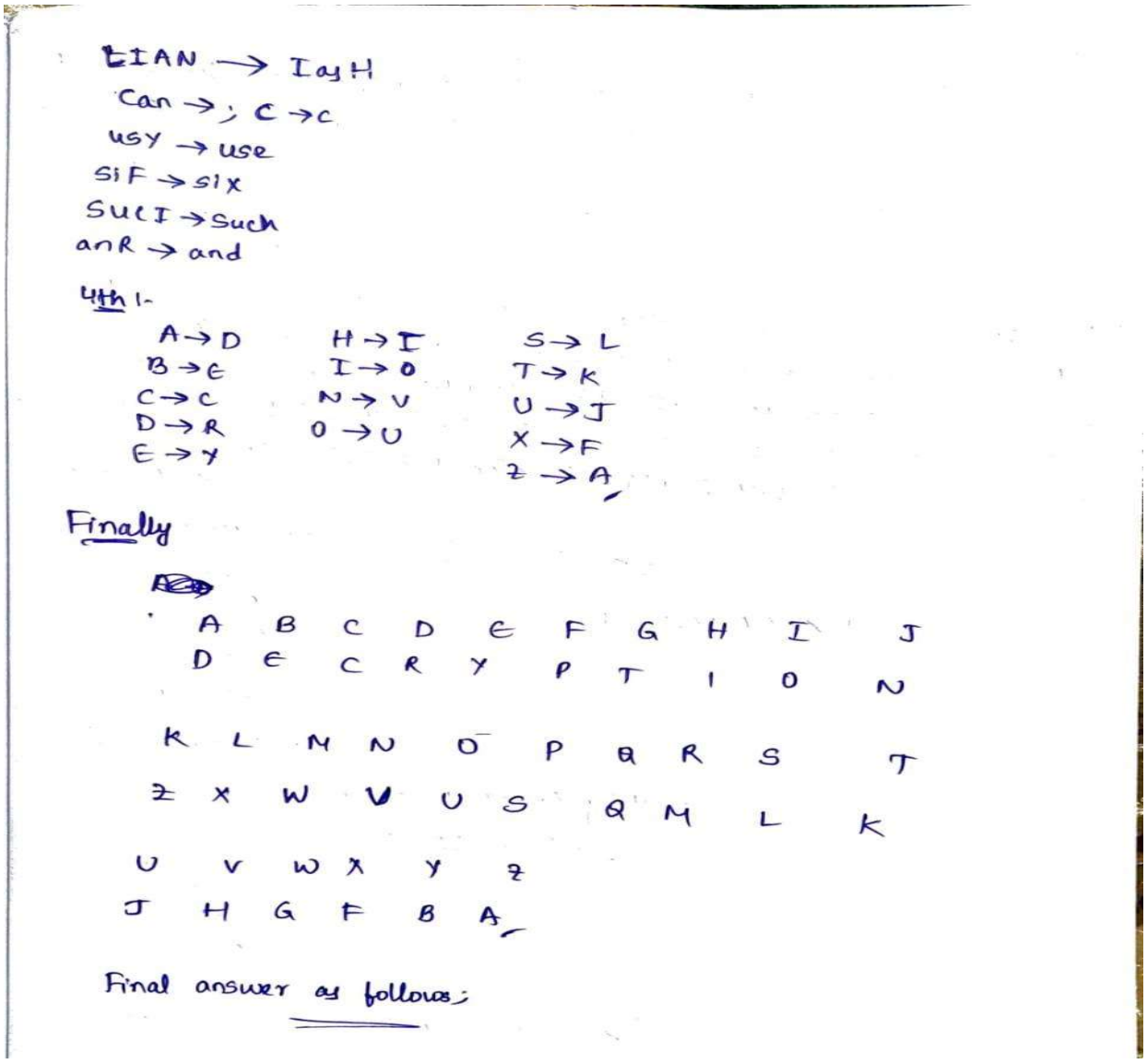
2nd guess :-

A → D
I → O
O → U
Z → A,

from word; LJELKOKJKOV → 'SUBSTITUTION'

3rd,

A → D
B → E
I → O
N → V
O → U
S → L
T → K
U → I
Z → A



Answer :

A SUBSTITUTION CIPHER IS HARDER TO CRACK THAN A CAESAR CIPHER BUT WE CAN STILL USE FREQUENCY ANALYSIS TO FIND THE MOST COMMON LETTERS. I PROMISED YOU THAT I WOULD USE ALL TWENTY SIX LETTERS SO THAT MEANS THAT I HAVE GOT TO ADD EXTRA WORDS SUCH AS JELLY AND ZOO.