Janvi Bhalala

Information & Network Security
(INS)– 2160711

Lab Manual

Semester 7th

Academic Year 2020-21 Odd

VVP Engineering College,
Rajkot

Gujarat Technological
University

Table of Contents

Practical 1

BREAKING THE SHIFT CIPHER

Step To Breaking the shift cipher

STEP 1 : For the given ciphertext in the **PART I** of the simulation page, the first step is to decrypt it using each of the twenty-six different keys, k=0,1,...,25 and obtain the corresponding plaintexts. For decryption, you may use the tool given in the **PART III** of the simulation page.

STEP 2 : After each decryption, you may cut-and-paste the resultant plaintext in the scratch-pad in the **(PART II)** of the simulation page, if you need to remember it.

STEP 3 : Finally, observe the plaintexts and choose the most appropriate one (the one that is a meaningful English text) as the recovered plaintext and cut-and-paste it in the text-field named **PART IV** "Solution Plaintext". Also select the corresponding key in the text-field named "Key" and click on "Check My answer" Button.

STEP 4 [OPTIONAL] : Verify that your answer is correct, by encrypting the solution plaintext with your key.

Example:

Given a cipher text, find out the corresponding plain text using brute force attack.

Ciphertext: HAAHJR HA KHDU

For k=0

Cipher text: HAAHJR HA KHDU
plain text: haahjr ha khdu

For k=1

Cipher text: HAAHJR HA KHDU
plain text: fyyfhp fy ifbs

For k=2

Cipher text: HAAHJR HA KHDU
plain text: fyyfhp fy ifbs

For k=3

Cipher text: HAAHJR HA KHDU
plain text: exxego ex hear

For k=4

Ciphertext: HAAHJR HA KHDU
plain text: dwwdfn dw gdzq

For k=5

Ciphertext: HAAHJR HA KHDU
plain text: cvvcem cv fcyp

For k=6

Ciphertext: HAAHJR HA KHDU
plain text: buubdl bu ebxo

For k=7

Ciphertext: HAAHJR HA KHDU
plain text: attack at dawn

For k=7, we obtain a meaningful plain text namely **attack at dawn** and hence we are done.

Practical 2

BREAKING THE MONOALPHABETIC SUBSTITUTION CIPHER

STEP 1 : For the given ciphertext in the **PART I** of the experiment page, the first step is to generate ciphertext by clicking on the "Next CipherText" button.

STEP 2 : Calculate frequencies of generated ciphertext by clicking on "Calculate Frequencies in Ciphertext" button

STEP 3 : Copy the generated ciphertext from **PART I** and paste in "Scratchpad" area of **PART II**

STEP 4 : Analyse similarties between "Calculated Frequencies Table" and "English Alphabet Frequencies Table"

STEP 5 : Based on similarities,try to make a frequency based estimation for each character of ciphertext

STEP 6 : Replace characters of CipherText in Scratchpad with a character estimated previously using a **Modify** function of **PART II**

STEP 7 : Based on Hints from Ciphertext in "Scratchpad" area make more replacement of ciphertext characters

STEP 8 : Repeat **Step 7** till you get a meaningful English Text

STEP 9 : Finally, observe the deciphered plaintext in Scratchpad Area,if a meaningful English text is formed cut-and-paste it in the text-field named "Solution Plaintext" of **PART III**. Also enter the final character mapping in the"Solution Key" in **PART III** and click on "Check Answer" button.

STEP 10[OPTIONAL] : Verify that your answer is correct, by encrypting the solution plaintext with your key in **PART IV**.

Example:

CypherText

awbix ildxz kolf a dkzeplld afu zbjjbfm lf bj bz a rwkx iajxpobwwap zdlgbfm a ellgae. jex iajxpobwwap ykxzjblfz awbix afu zex audbjz jl exp ikppxfj buxfjbjt ipbzbz, ildolkfuxu rt exp bfarbwbjt jl pxdxdrxp a olxd. rxnlpx ipahwbfm ahat, jex iajxpobwwap jxwwz awbix jeaj lfx zbux ln jex dkzeplld hbww dagx exp jawwxp afu jex ljexp zbux hbww dagx exp zelpjxp. zex rpxagz lnn jhl obxixz npld jex dkzeplld. lfx zbux dagxz exp zepbfg zdawwxp jeaf xcxp, hebwx afljexp iakzxz exp fxig jl mplh ebme bfjl jex jpxxz, hexpx a obmxlf dbzjagxz exp nlp a zxpoxfj. hbje zldx xnnlpj, awbix rpbfmz expzxwn raig jl

exp kzkaw exbmej. zex zjkdrwxz kolf a zdaww xzjajx afu kzxz jex dkzeplld jl pxaie a dlpx aooplopbajx exbmej.

CT	Frequency	PT
a	8.084	A
b	6.854	I
c	0.176	V
d	4.394	M
e	7.206	H
f	4.394	N
g	1.757	K
h	1.582	W
i	2.988	C
j	7.909	T
k	2.636	U
l	7.381	O
m	1.582	G
n	1.582	F
o	2.285	P
p	8.26	R
q	0	J
r	1.582	B
s	0	X
t	0.703	Y
u	1.933	D
v	0	Z
w	5.097	L
x	14.06	E
y	0.176	Q
z	7.381	S

Plain Text :

ALICE COMES UPON A MUSHROOM AND SITTING ON IT IS A BLUE CATERPILLAR SMOKING A HOOKAH. THE CATERPILLAR QUESTIONS ALICE AND SHE ADMITS TO HER CURRENT IDENTITY CRISIS, COMPOUNDED BY HER INABILITY TO REMEMBER A POEM. BEFORE CRAWLING AWAY, THE CATERPILLAR TELLS ALICE THAT ONE SIDE OF THE MUSHROOM WILL MAKE HER TALLER AND THE OTHER SIDE WILL MAKE HER SHORTER. SHE BREAKS OFF TWO PIECES FROM THE MUSHROOM. ONE SIDE MAKES HER SHRINK SMALLER THAN EVER, WHILE ANOTHER CAUSES HER NECK TO GROW HIGH INTO THE TREES, WHERE A PIGEON MISTAKES HER FOR A SERPENT. WITH SOME EFFORT, ALICE BRINGS HERSELF BACK TO HER USUAL HEIGHT. SHE STUMBLES UPON A SMALL ESTATE AND USES THE MUSHROOM TO REACH A MORE APPROPRIATE HEIGHT.