

Homework 0 - Breaking Codes and Learning Latex

Jubeen Shah

August 2019

Problem: Decrypt the following text

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXB-
JYUXJ LBJ00 KCPK. CP LBO LBCMCKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: "DJOXL EYPD,
ICJ X LBCMCKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACM-
PLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK
CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X
IXNCMJ CI UCMJ SXGOKLU?"

OFYRCDMO, LXROK IJCS LBO LBCMCKXPV XPV CPO PYDBLK

Solution

First frequency analysis of the text was performed, which gave the below table as a result

Letter	Frequency	Letter	Frequency
A	0.89%	B	7.44%
C	8.04%	D	4.17%
E	1.49%	F	0.6%
G	0.3%	I	3.27%
J	5.36%	K	7.74%
L	7.44%	M	3.27%
N	0.89%	O	10.71%
P	9.23%	Q	0.6%
R	1.79%	S	2.08%
U	1.79%	V	5.36%
W	0.3%	X	10.12%
Y	5.65%	Z	1.49%

From this we can gauge that top 3 most frequently used characters are X, O, and P. Based on the frequency table from the book we can assume the following.

$$\begin{aligned} X &= E \text{ or } T \text{ or } A \\ O &= E \text{ or } T \text{ or } A \\ P &= E \text{ or } T \text{ or } A \end{aligned}$$

From the text we also see that letters ‘OO’ exists, where as ‘XX’ does not; from which we can assume that O = E. X and Y each exists on their own throughout the text, from which we can assume, that X = A; and Y = I.

Therefore, we have the following.

$$\begin{aligned} X &= A \\ O &= E \\ Y &= I \end{aligned}$$

The text after substitution is as follows.

PCQ VMJIPD LBIK LISE KBABJAWAV BAV ZCJPE EIPD KBABJI-
UAJ LBJEE KCPK. CP LBE LBCM KAPV APV IJJKL PIDBL, QBEP
KBE BAV EPVEV LBE LARE CI SA’AJMI, KBE JCKE APV EIKKEV
LBE DJCMPV ZEICJE BIS, KAUIPD: “DJEAL EIPD, ICJ A LBCM KAPV
APV CPE PIDBLK I BANE ZEEP JEACMPLIPD LC UCM LBE IAZREK
CI FAKL ADEK APV LBE REDEPVK CI APAIEPL EIPDK. SAU I
SAEE KC ZCRV AK LC AJANE A IANCMJ CI UCMJ SAGEKLU?”
EFIRCDME, LAREK IJCS LBE LBCM KAPV APV CPE PIDBLK

The trigram ‘APV’ repeats at least 8 times, which could be ‘AND’. Hence we assume,

$$\begin{aligned} P &= N \\ V &= D \\ B &= H \end{aligned}$$

The text after substitution is as follows.

NCQ DMJIND LHIK LISE KHAHJAWAD HAD ZCJNE EIND KHAHJI-
UAJ LHJEE KCNK. CN LHE LHCMKAND AND IJJKL NIDHL, QHEN
KHE HAD ENDED LHE LARE CI SA’AJMI, KHE JCKE AND EIKKED
LHE DJCMND ZEICJE HIS, KAUIND: “DJEAL EIND, ICJ A LHCMKAND
AND CNE NIDHLK I HANE ZEEN JEACMNLIND LC UCM LHE
IAZREK CI FAKL ADEK AND LHE REDENDK CI ANAIENL EINDK.
SAU I SAEE KC ZCRD AK LC AJANE A IANCMJ CI UCMJ SAGEKLU?”
EFIRCDME, LAREK IJCS LHE LHCMKAND AND CNE NIDHLK

Looking the words like ‘NCQ’, might translate to ‘NOW’, ‘KHE’ might translate to ‘THE’ or ‘SHE’ which leads to assume that

$$\begin{aligned} C &= O \\ Q &= W \\ L &= T \text{ or } K = T \\ K &= S \text{ or } K = ? \end{aligned}$$

When making the substitutions we get the following text,

NOW DMJIND THIS TISE SHAHJAWAD HAD ZOJNE EIND SHAHJI-
UAJ THJEE SONS. ON THE THOMSAND AND IJST NIDHT, WHEN
SHE HAD ENDED THE TARE OI SA'AJMI, SHE JOSE AND EISSED
THE DJOMND ZEIOJE HIS, SAUIND: "DJEAT EIND, IOJ A THOM-
SAND AND ONE NIDHTS I HANE ZEEN JEAOMNTIND TO UOM
THE IAZRES OI FAST ADES AND THE REDENDS OI ANAIENT
EINDS. SAU I SAE SO ZORD AS TO AJANE A IANOMJ OI UOMJ
SAGESTU?"

EFIRODME, TARES IJOS THE THOMSAND AND ONE NIDHTS

The word 'THOMSAND' might translate to 'THOUSAND', 'NIDHTS' might
translate to 'NIGHTS' assuming $M = U$ and $D = G$.

NOW DMJIND THIS TISE SHAHJAWAD HAD ZOJNE EIND SHAHJI-
UAJ THJEE SONS. ON THE THOMSAND AND IJST NIDHT, WHEN
SHE HAD ENDED THE TARE OI SA'AJMI, SHE JOSE AND EISSED
THE DJOMND ZEIOJE HIS, SAUIND: "DJEAT EIND, IOJ A THOU-
SAND AND ONE NIGHTS I HANE ZEEN JEAOMNTIND TO UOM
THE IAZRES OI FAST ADES AND THE REDENDS OI ANAIENT
EINDS. SAU I SAE SO ZORD AS TO AJANE A IANOMJ OI UOMJ
SAGESTU?"

EFIRODME, TARES IJOS THE THOUSAND AND ONE NIGHTS

Continuing the process I found the following substitution for the letters.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XZAVOIDBYGERSPCFHJKLMNQUTW

NOW DURING THIS TIME SHAHRAZAD HAD BORNE KING SHAHRI-
YAR THREE SONS. ON THE THOUSAND AND FIRST NIGHT, WHEN
SHE HAD ENDED THE TALE OF MA'ARUF, SHE ROSE AND KISSED
THE GROUND BEFORE HIM, SAYING: "GREAT KING, FOR A THOU-
SAND AND ONE NIGHTS I HAVE BEEN RECOUNTING TO YOU
THE FABLES OF PAST AGES AND THE LEGENDS OF ANCIENT
KINGS. MAY I MAKE SO BOLD AS TO CRAVE A FAVOUR OF YOUR
MAJESTY?"

EPILOGUE, TALES FROM THE THOUSAND AND ONE NIGHTS