

NAME: Mayuri Shridatta Yerande
ROLL NO: 61
CLASS:D15B

CNS EXPERIMENT - 1

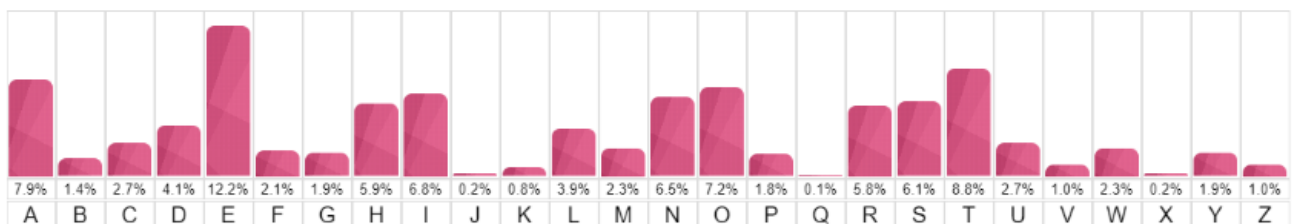
AIM: To understand the process of Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method.

THEORY:

- A monoalphabetic substitution is a **cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext**. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.
- Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.
- The relationship between a character in the plain text and the characters in the ciphertext is one-to-one.
- Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.
- A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.
- It includes additive, multiplicative, affine and monoalphabetic substitution cipher.
- It is a simple substitution cipher.
- Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.
- Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.

IMPLEMENTATION:

The Given Frequency Graph:

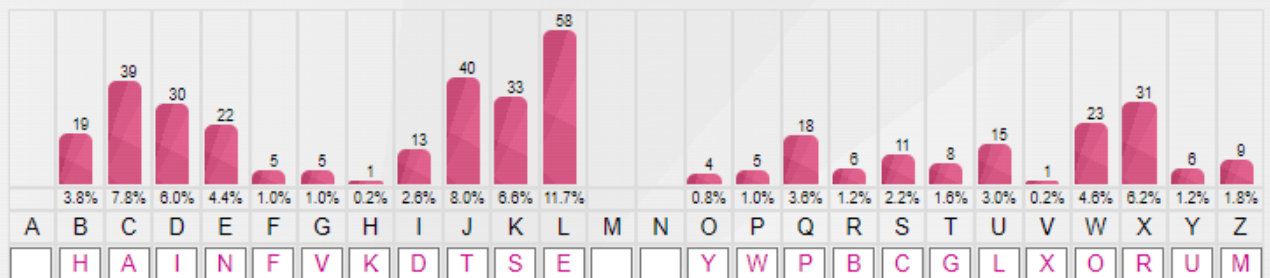


CIPHER 1:

The Given Text:

text:
DJ DK C QLXDWI WF SDGDU PCX. XLRLU KQCSLKBDQK, KJXDHDET FXWZ C BDIILE RCKL, BCGL
PWE JBLDX FDXKJ GDSJWXO CTCDEKJ JBL LGDU TCUCSJDS LZQDXL. IYXDET JBL RCJJUL,
XLRLU KQDLK ZCECTLI JW KJLCU KLSXLJ QUCEK JW JBL LZQDXL'K YUJDZCJL PLCQWE, JBL
ILCJB KJCX, CE CXZWXLI KQCSL KJCJDWE PDJB LEWYTB QWPLX JW ILKJXWO CE LEJDXL
QUCELJ. QYXKYLI RO JBL LZQDXL'K KDEDKJLX CTLEJK, QXDESLKK ULDC XCSLK BWZL CRWCXI
BLX KJCXKBDQ, SYKJWIDCE WF JBL KJWULE QUCEK JBCJ SCE KCGL BLX QLWQUL CEI XLKJWXL
FXLLIWZ JW JBL TCUCVO...

Text Substitution after Analysis:



2. Start Substitution

Text After Substitution:

IT IS A PERIOD OF CIVIL WAR. REBEL SPACESHIPS, STRIKING FROM A HIDDEN BASE, HAVE
WON THEIR FIRST VICTORY AGAINST THE EVIL GALACTIC EMPIRE. DURING THE BATTLE,
REBEL SPIES MANAGED TO STEAL SECRET PLANS TO THE EMPIRE'S ULTIMATE WEAPON, THE
DEATH STAR, AN ARMORED SPACE STATION WITH ENOUGH POWER TO DESTROY AN ENTIRE
PLANET. PURSUED BY THE EMPIRE'S SINISTER AGENTS, PRINCESS LEIA RACES HOME ABOARD
HER STARSHIP, CUSTODIAN OF THE STOLEN PLANS THAT CAN SAVE HER PEOPLE AND RESTORE
FREEDOM TO THE GALAXY...

CIPHER 2

Frequency Analysis

Text:

JVUI LUMNCJUIG KCL GIXVGEIS XO KPL KOYI AJCEIX OQ XCXOOPEI PE CE CXXIYAX XO GILWVI KPL QGPIES KCE LOJO QGOY XKI WJVXWKIL OQ XKI DPJI TCETLXIG BCHHC XKI KVXX. JPXXJI SOIL JVUI UEON XKCX XKI TCJCWXPW IYAPGI KCL LIWGIXJM HITVE WOELXGVWXPOE OE C EIN CGYOGIS LACWI LXCXPOE IDIE YOGI AONIGQVJ XKCE XKI QPGLX SGICISIS SICXK LXCG. NKIE WOYAJIXIS, XKPL VJXPYCXI NICAOE NPJJ LAIJU WIGXCPE SOOY QOG XKI LYCJJ HCES OQ GIHIJL LXGVTTJPET XO GILXOGI QGIISOY XO XKI TCJCZM..

1. Start Frequency Analysis

8	1	29	2	22		24	5	52	23	20	22	3	7	29	17	9		12	8	5	11	11	43	11	1
8%	0.2%	6.4%	0.4%	4.8%		5.3%	1.1%	11.4%	5.0%	4.4%	4.8%	0.7%	1.5%	6.4%	3.7%	2.0%		2.6%	1.8%	1.1%	2.4%	2.4%	9.4%	2.4%	0.2%
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
P	J	A	V	N		R	B	E	L	H	S	Y	W	O	I	F		D	G	K	U	C	T	M	X

2. Start Substitution

Text After Substitution:

LUKE SKYWALKER HAS RETURNED TO HIS HOME PLANET OF TATOOINE IN AN ATTEMPT TO RESCUE HIS FRIEND HAN SOLO FROM THE CLUTCHES OF THE VILE GANGSTER JABBA THE HUTT. LITTLE DOES LUKE KNOW THAT THE GALACTIC EMPIRE HAS SECRETLY BEGUN CONSTRUCTION ON A NEW ARMORED SPACE STATION EVEN MORE POWERFUL THAN THE FIRST DREADED DEATH STAR. WHEN COMPLETED, THIS ULTIMATE WEAPON WILL SPELL CERTAIN DOOM FOR THE SMALL BAND OF REBELS STRUGGLING TO RESTORE FREEDOM TO THE GALAXY...

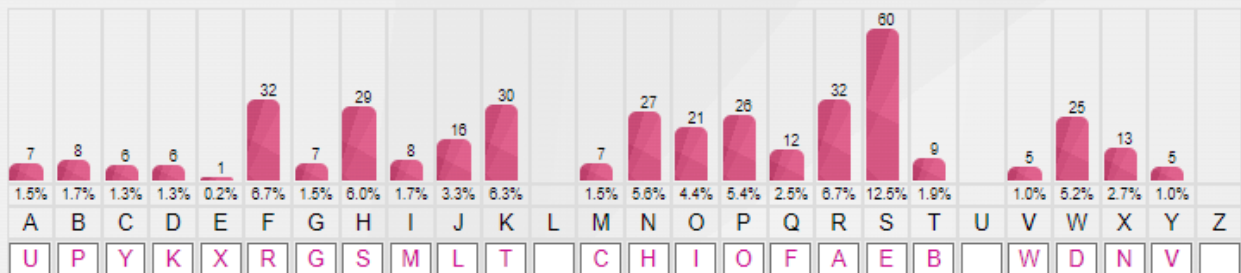
CIPHER 3

Frequency Analysis

Text:

OK OH R WRFD KOIS QFF KNS FSTSJJOPX. RJKNPAGN KNS WSRKN HKRF NRH TSSX WSHKFPCSW,
OIBSFORJ KFPFBH NRYS WFOYSX KNS FSTSJ QPFMSH QFPI KNSOF NOWWSX TRHS RXW BAFHASW
KNSI RMFPFH KNS GRJREC.
SYRWOXG KNS WFSRWSW OIBSFORJ HKRFQJSSK, R GFPAB PQ QFSSWPI QOGNKSFH JSW TC JADS
HDCVRJDSF NRH SHKRIJOHNSW R XSV HSMFSK TRHS PX KNS FSIPKS OMS VPFJW PQ NPKN.
KNS SYOJ JPFW WRFKN YRWSE, PTHSHHSW VOKN QOXWOXG CPAXG HDCVRJDSF, NRH WOHBKMNWSW
KNPAHRXWH PQ FSIPKS BFPTSH OXKP KNS QRF FSRMNSH PQ HBRMS...

1. Start Frequency Analysis



2. Start Substitution

Text After Substitution:

IT IS A DARK TIME FOR THE REBELLION. ALTHOUGH THE DEATH STAR HAS BEEN DESTROYED,
IMPERIAL TROOPS HAVE DRIVEN THE REBEL FORCES FROM THEIR HIDDEN BASE AND PURSUED
THEM ACROSS THE GALAXY.
EVADING THE DREADED IMPERIAL STARFLEET, A GROUP OF FREEDOM FIGHTERS LED BY LUKE
SKYWALKER HAS ESTABLISHED A NEW SECRET BASE ON THE REMOTE ICE WORLD OF HOTH.
THE EVIL LORD DARTH VADER, OBSESSED WITH FINDING YOUNG SKYWALKER, HAS DISPATCHED
THOUSANDS OF REMOTE PROBES INTO THE FAR REACHES OF SPACE...

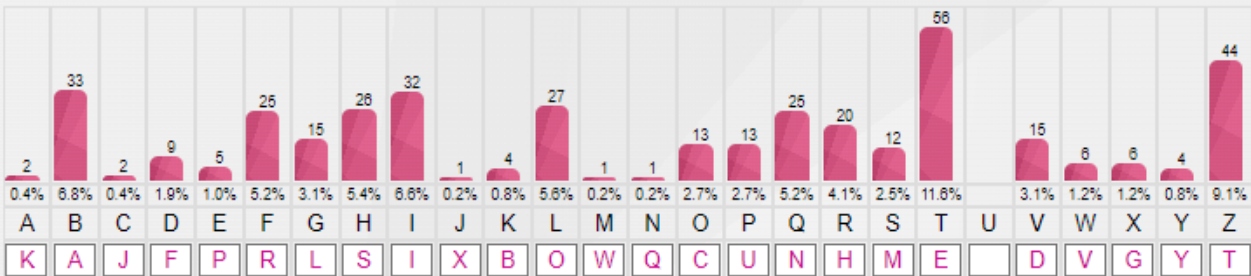
CIPHER 4

Frequency Analysis

Text:

ZRTFT IH PQFTHZ IQ ZRT XBGBOZIO HTQBZT. HTWTFBG ZRLPHBQV HLGBF HYHZTSH RBWT
VTOGBFTV ZRTIF IQZTQZILQH ZL GTBWT ZRT FTEPKGIO.
ZRIH HTEBFBZINH SLWTSTQZ, PQVTF ZRT GTBVTFHRIE LD ZRT SYHZTFILPH OLPQZ VLLAP, RBH
SBVT IZ VIDDIOPGZ DLF ZRT GISIZTV QPSKTF LD CTVI AQIXRZH ZL SBIQZBIQ ETBOT BQV
LFVTF IQ ZRT XGBBJY.
HTQBZLF BSIVBGB, ZRT DLFSTF NPTTQ LD QBKLL, IH FTZPFQIQX ZL ZRT XBGBOZIO HTQBZT
ZL WLZT LQ ZRT OFIZIOBG IHHFT LD OFTBZIQX BQ BFSY LD ZRT FTEPKGIO ZL BHHIHZ ZRT
LWTFMRTGSTV CTVI...

1. Start Frequency Analysis



2. Start Substitution

Text After Substitution:

THERE IS UNREST IN THE GALACTIC SENATE. SEVERAL THOUSAND SOLAR SYSTEMS HAVE
DECLARED THEIR INTENTIONS TO LEAVE THE REPUBLIC.
THIS SEPARATIST MOVEMENT, UNDER THE LEADERSHIP OF THE MYSTERIOUS COUNT DOOKU, HAS
MADE IT DIFFICULT FOR THE LIMITED NUMBER OF JEDI KNIGHTS TO MAINTAIN PEACE AND
ORDER IN THE GALAXY.
SENATOR AMIDALA, THE FORMER QUEEN OF NABOO, IS RETURNING TO THE GALACTIC SENATE
TO VOTE ON THE CRITICAL ISSUE OF CREATING AN ARMY OF THE REPUBLIC TO ASSIST THE
OVERWHELMED JEDI...

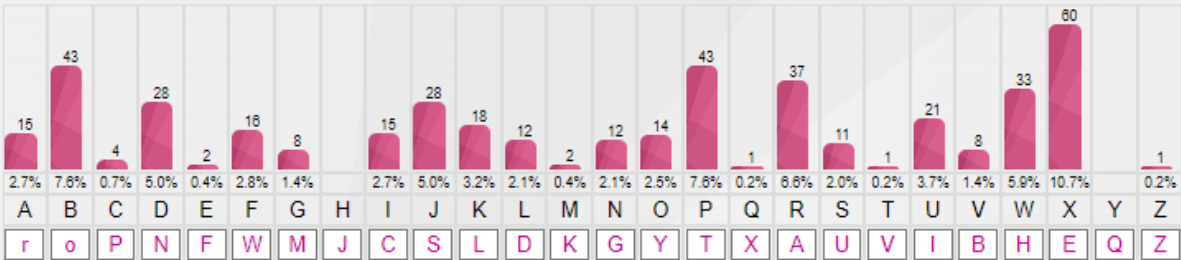
CIPHER 5

Frequency Analysis

Text:

FX IWBBJX PB NB PB FWX GBBD. VSP FWO, JBGX JRO, FWX GBBD? FWO IWBBJX PWUJ RJ BSA
NBRK? RDL PWXO GRO FXKK RJM FWO IKUGV FWX WUNWXJP GBSDEPRUD? FWO, 35 OXRAJ RNB,
EKO FWX RPKRDPUI? FWO LBXJ AUIX CKRO FXQRJ? FX IWBBJX PB NB PB FWX GBBD UD PWUJ
LXIRLX RDL LB PWX BPWA PWUDNJ, DBP VXIRSJX PWXO RAX XRJO, VSP VXIRSJX PWXO RAX
WRAL, VXIRSJX PWRP NBRK FUKK JXATX PB BANRDUZX RDL GXRJSAX PWX VXJP BE BSA
XDXANUXJ RDL JMUUKJ, VXIRSJX PWRP IWRKKXDNX UJ BDX PWRP FX RAX FUKKUDN PB RIIXCP,
BDX FX RAX SDFUKKUDN PB CBJPCBDX, RDL BDX FWUIW FX UDPXDL PB FUD, RDL PWX BPWXAJ,
PBB.

1. Start Frequency Analysis



2. Start Substitution

Text After Substitution:

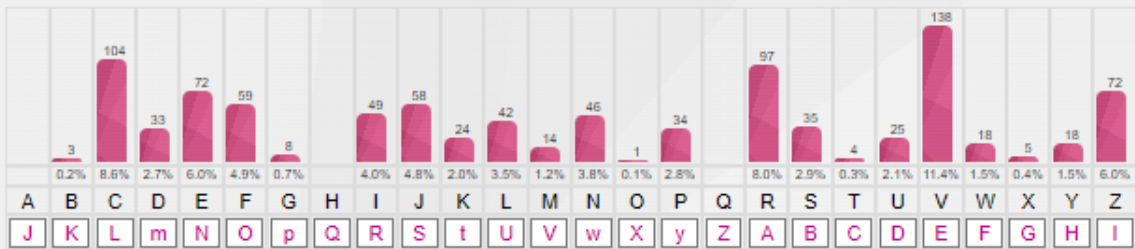
WE CHOOSE TO GO TO THE MOON. BUT WHY, SOME SAY, THE MOON? WHY CHOOSE THIS AS OUR
GOAL? AND THEY MAY WELL ASK WHY CLIMB THE HIGHEST MOUNTAIN? WHY, 35 YEARS AGO,
FLY THE ATLANTIC? WHY DOES RICE PLAY TEXAS? WE CHOOSE TO GO TO THE MOON IN THIS
DECADE AND DO THE OTHER THINGS, NOT BECAUSE THEY ARE EASY, BUT BECAUSE THEY ARE
HARD, BECAUSE THAT GOAL WILL SERVE TO ORGANIZE AND MEASURE THE BEST OF OUR
ENERGIES AND SKILLS, BECAUSE THAT CHALLENGE IS ONE THAT WE ARE WILLING TO ACCEPT,
ONE WE ARE UNWILLING TO POSTPONE, AND ONE WHICH WE INTEND TO WIN, AND THE OTHERS,
TOO.

CIPHER 6

Given Text:

"ZE KYV KFNE NYVIV Z NRJ SFIE
CZMVU R DRE NYF JRZCVU KF JVR
REU YV KFCU LJ FW YZJ CZWV
ZE KYV CREU FW JLSDRIZEVJ
JF NV JRZCVU LG KF KYV JLE
'KZC NV WFLEU R JVR FWXIVVE
REU NV CZMVU SVEVRKY KYV NRMVJ
ZE FLI PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
REU FLI WIZVEUJ RIV RCC RSFRIU
DREP DFIV FW KYVD CZMV EVOK UFFI
REU KYV SREU SVXZEJ KF GCRP
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
(WLCC JGVVU RYVRU DI. GRIBVI, WLCC JGVVU RYVRU
WLCC JGVVU RYVRU ZK ZJ, JVIXVREK
RTKZFE JKRKZFE, RTKZFE JKRKZFE
RPV, RPV, JZI, WZIV
TRGKRZE, TRGKRZE)
RJ NV CZMV R CZWV FW VRJV
VMVIPFEV FW LJ YRJ RCC NV EVVU (YRJ RCC NV EVVU)
JBP FW SCLV (JBP FW SCLV) REU JVR FWXIVVE (REU JVR FWXIVVE)
ZE FLI PVCCFN JLSDRIZEV (ZE FLI PVCCFN, JLSDRIZEV, YR YR)
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV
NV RCC CZMV ZE R PVCCFN JLSDRIZEV
PVCCFN JLSDRIZEV, PVCCFN JLSDRIZEV"

Text After Substitution:



2. Start Substitution

Text After Substitution:

IN THE TOWN WHERE I WAS BORN
LIVED A MAN WHO SAILED TO SEA
AND HE TOLD US OF HIS LIFE
IN THE LAND OF SUBMARINES
SO WE SAILED UP TO THE SUN
'TIL WE FOUND A SEA OF GREEN
AND WE LIVED BENEATH THE WAVES
IN OUR YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE

Text After Substitution:

AND OUR FRIENDS ARE ALL ABOARD
MANY MORE OF THEM LIVE NEXT DOOR
AND THE BAND BEGINS TO PLAY
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
(FULL SPEED AHEAD MR. PARKER, FULL SPEED AHEAD
FULL SPEED AHEAD IT IS, SERGEANT
ACTION STATION, ACTION STATION
AYE, AYE, SIR, FIRE
CAPTAIN, CAPTAIN)

Text After Substitution:

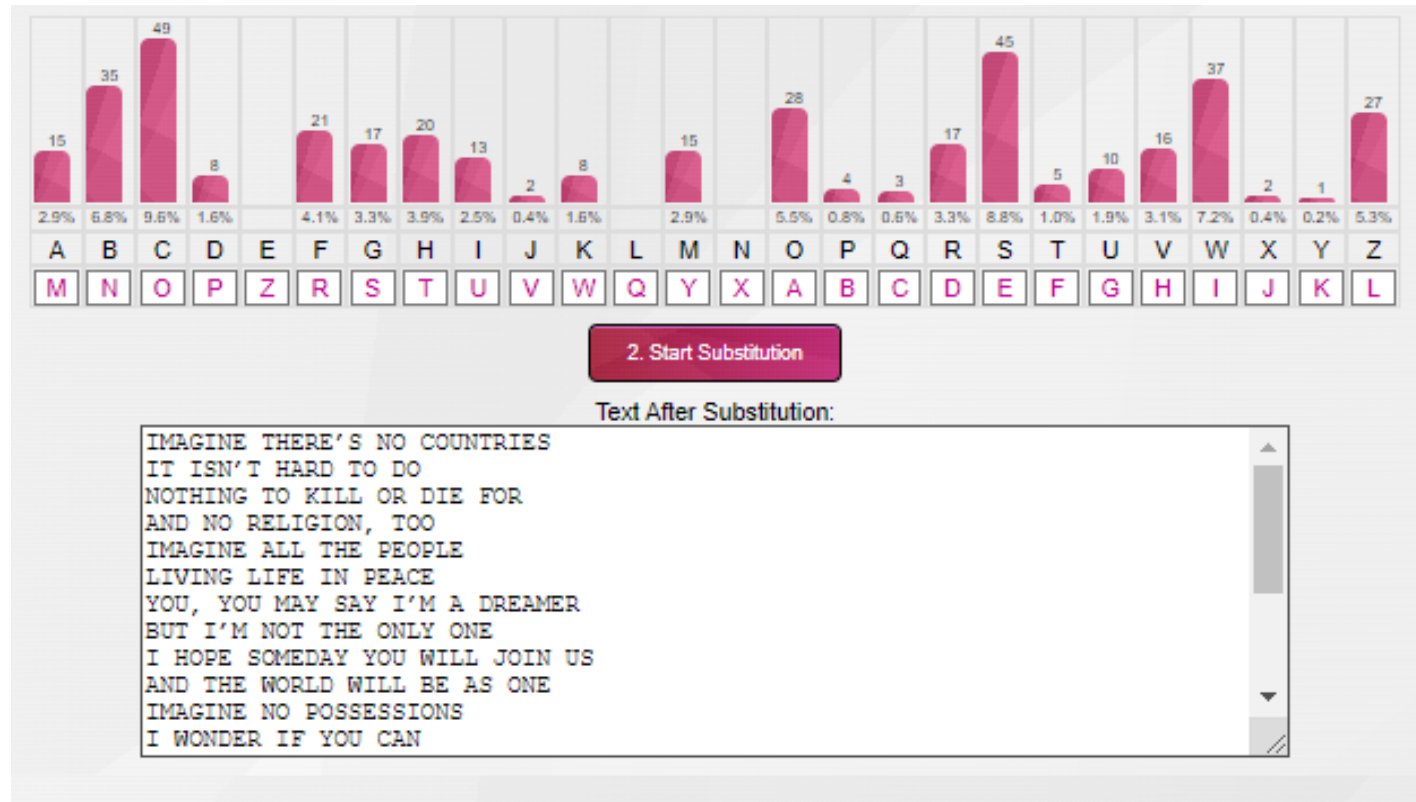
AS WE LIVE A LIFE OF EASE
EVERYONE OF US HAS ALL WE NEED (HAS ALL WE NEED)
SKY OF BLUE (SKY OF BLUE) AND SEA OF GREEN (AND SEA OF GREEN)
IN OUR YELLOW SUBMARINE (IN OUR YELLOW, SUBMARINE, HA HA)
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE
WE ALL LIVE IN A YELLOW SUBMARINE
YELLOW SUBMARINE, YELLOW SUBMARINE

CIPHER 7

Given Text:

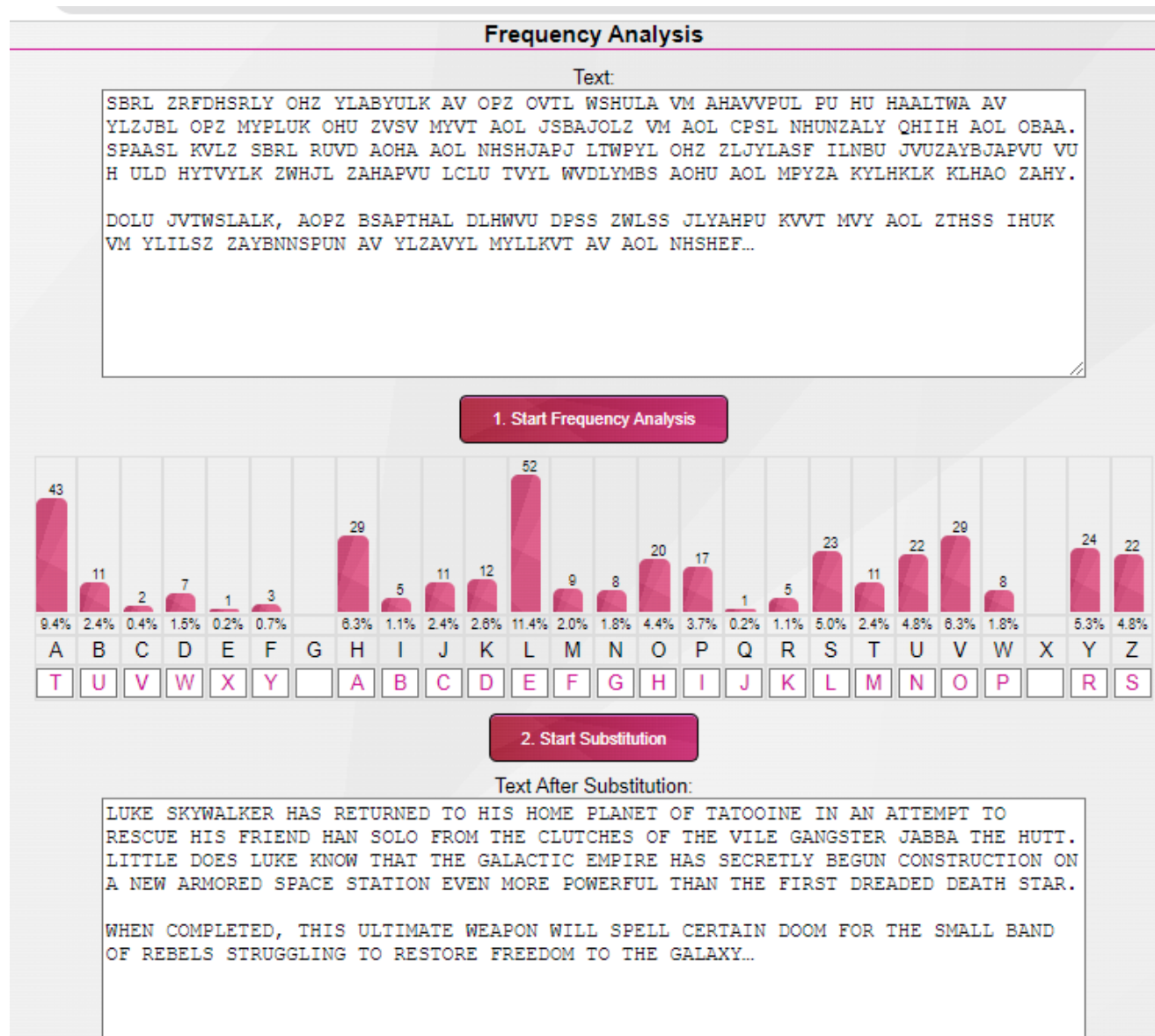
"WAOUWBS HV'SFS'G BC QCIBHFW'SG
WH WGB'H VOFR HC RC
BCH'WBU HC YWZZ CF RWS TCF
OBR BC FSZWUWCB, HCC
WAOUWBS OZZ HVS DSCDZS
ZWJWBU ZWTS WB DSOQS
MCI, MCI AOM GOM W'A O RFSOASF
PIH W'A BCH HVS CBZM CBS
W VCDS GCASROM MCI KWZZ XCWB IG
OBR HVS KCFZR KWZZ PS OG CBS
WAOUWBS BC DCGGSGGWCBG
W KCBRSF WT MCI QOB
BC BSSR TCF UFSSR CF VIBUSF
O PFCHVSFVCCR CT AOB
WAOUWBS OZZ HVS DSCDZS
GVOFWBU OZZ HVS KCFZR
MCI, MCI AOM GOM W'A O RFSOASF
PIH W'A BCH HVS CBZM CBS
W VCDS GCASROM MCI KWZZ XCWB IG
OBR HVS KCFZR KWZZ ZWJS OG CBS"

Text After substitution:



BUT I'M NOT THE ONLY ONE
I HOPE SOMEDAY YOU WILL JOIN US
AND THE WORLD WILL BE AS ONE
IMAGINE NO POSSESSIONS
I WONDER IF YOU CAN
NO NEED FOR GREED OR HUNGER
A BROTHERHOOD OF MAN
IMAGINE ALL THE PEOPLE
SHARING ALL THE WORLD
YOU, YOU MAY SAY I'M A DREAMER
BUT I'M NOT THE ONLY ONE
I HOPE SOMEDAY YOU WILL JOIN US

CIPHER 8



CONCLUSION: Process of Breaking the Mono-alphabetic Substitution Cipher using Frequency analysis method is successfully implemented.