

Name	Shubham Solanki
UID	2022301015
Experiment number	1
Title	Implement different substitution techniques
Batch	VIII (Comps A)

## 1.Caesar Cipher

**Plain text** - Believe in the power of your dreams. Every step forward, no matter how small, brings you closer to your goals. Embrace the challenges and celebrate the progress. You are stronger and more capable than you know. Keep pushing forward with passion and resilience—your future self will thank you.

**Cipher text** - ZcJgctc gl rfc nmucp md wmsp bpcykq. Ctcpw qrcn dmpuypb, lm kyrrcp fmu qkyjj, zpgleq wms ajmqcp rm wmsp emyjq. Ckzpyac rfc afyjjclecq ylb acjczpyrc rfc npmepcqq. Wms ypc qrpmlecp ylb kmpe ayxyzjc rfyl wms ilmu. Iccn nsqfgle dmpuypb ugrf nyqqgml ylb pcqggjclac wmsp dsrspc qcjd ugjj rfyli wms.

**Key** - 50

```

USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/caesarCipher
• $ python caesarCipher.py
Select the operation you want to perform.

1. Encrypt
2. Decrypt

Your choice: 1
Encryption completed successfully.

USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/caesarCipher
• $ python caesarCipher.py
Select the operation you want to perform.

1. Encrypt
2. Decrypt

Your choice: 2
Decryption completed successfully.

```

```

plain-text.txt •
substitution-techniques > caesarCipher > plain-text.txt
1  50
2  Believe in the power of your dreams. Every step forward, no matter how small, brings you closer to your goals.
3  Embrace the challenges and celebrate the progress. You are stronger and more capable than you know.
4  Keep pushing forward with passion and resilience your future self will thank you.

```

```

cipher-text.txt •
substitution-techniques > caesarCipher > cipher-text.txt
1  50
2  ZcJgctc gl rfc nmucp md wmsp bpcykq. Ctcpw qrcn dmpuypb, lm kyrrcp fmu qkyjj, zpgleq wms ajmqcp rm wmsp emyjq.
3  Ckzpyac rfc afyjjclecq ylb acjczpyrc rfc nmepcqq. Wms ypc qrpmlecp ylb kmpe aynyzjc rfyl wms ilmu.
4  Iccn nsqfgle dmpuypb ugrf nyqqgm1 ylb pcqgjgclac wmsp dsrspc qcjd ugjj rfyli wms.

```

```

outplain-text.txt X
substitution-techniques > caesarCipher > outplain-text.txt
1  50
2  Believe in the power of your dreams. Every step forward, no matter how small, brings you closer to your goals.
3  Embrace the challenges and celebrate the progress. You are stronger and more capable than you know.
4  Keep pushing forward with passion and resilience your future self will thank you.

```

## Attack

```

27 Mpwtpgp ty esp azhpc zq jzfc ocplxd. Pgpcj depa qzchlco, yz xleepc szh dxlww, mctyrd jzf nwzdpz ez jzfc rzlwd. Pxm
28
29 Lovsofo sx dro zygoz yp iyeb nbokwc. Ofobi cdoz pybgkbn, xy wkddob ryg cwkvv, lbsxqc iye mvycob dy iyeb qykvz. Owl
30
31 Knurnen rw cqn yxfna xo hxda manjvb. Nenah bcny oxafjam, wx vjccna qxf bvjuu, karwpb hxd luxbna cx hxda pxjub. Nvk
32
33 Jmtqmdm qv bpm xwemz wn gwcx lzmiua. Mdmzg abmx nwzeizl, vw uibbmz pwe auitt, jzqvoa gwc ktwamz bw gwcx owita. Muj
34
35 Ilspicl pu aol wvdly vm fvby kylhtz. Lclyf zalw mvydhyk, uv thaaly ovd zthss, iypunz fvb jsvzly av fvby nvhsz. Lti
36
37 Hkrokbn ot znk vuckx ul euax jxkgsy. Kbkxe yzkv luxcgxj, tu sgzzkx nuc ysgrr, hxotmy eua iruykx zu euax mugry. Ksh
38
39 Gjgnhaj ns ymj utbjw tk dtzw iwjfrx. Jajwd xyju ktwbfiw, st rfyjyw mtb xrfqq, gwnslx dtz hqtxjw yt dtzw ltfqx. Jrg
40
41 Fipmizi mr xli tsaiv sj csyv hvieqw. Izivc wxit jsvaevh, rs qexxiv lsa wqepz, fvmrkx csy gpswiv xs csyv ksepw. Iqf
42
43 Eholhyh lq wkh srzhu ri brxu guhdpv. Hyhub wvhs iruzdug, qr pdwwhu krz vpdoo, eulqjv brx forvhu wr brxu jrdov. Hpe
44
45 Dgnkgxg kp vjg rxygt qh aqwt ftgcou. Gxgta uvgr hqtyctf, pq ocvvgt jay uocnn, dtkpiu aqw enqutg vq aqwt iqcnv. God
46
47 Cfmjfwf jo uif qpxfs pg zpvz esfbnt. Fwfsz tufq gpxsbse, op nbuufs ipx tnbmm, csjoht zpv dmptfs up zpvz hpbmt. Fnc
48
49 Believe in the power of your dreams. Every step forward, no matter how small, brings you closer to your goals. Emb
50
51 Adkhduh hm sgd onvdq ne xntq cqdzlr. Dudqx rsdo enqvzqc, mn lzssdq gnv rlxkk, aqhmfr xnt bkndq sn xntq fnzkr. Dla

```

## 2. Monoalphabetic cipher

**Plain text** - Believe in the power of your dreams Every step forward no matter how small brings you closer to your goals Embrace the challenges and celebrate the progress You are stronger and more capable than you know Keep pushing forward with passion and resilience your future self will thank you

### Cipher text -

SGVDDWDSSPTFYPTMZBDHPZLGMGSQEMWDLOESCTGHMZBQCIT  
RSHSMQOTZEWIQRILBBCITPZDKTBGMHPTPZKRBIQEMRSQBDFHOF  
DAFQVMDBCMEBIEDDMGsQBsmHOCTZBRZMEITPZBQMEOMPBCFQ  
BICRTMGFNHNIRMSAFIPPZUCTZMCCTNPATSICGBZXSLGVSHOHNA  
WASPBBIGLMEDVSDCKDTPZQGWPZKMEDMEXDVMYAFcutpvz

## Key - pythonitis

```
USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/monoAlphabeticCipher
$ python monoAlphaCipher.py
Select the operation you want to perform.

1. Encrypt
2. Decrypt

Your choice: 1
Encryption completed successfully.

USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/monoAlphabeticCipher
$ python monoAlphaCipher.py
Select the operation you want to perform.

1. Encrypt
2. Decrypt

Your choice: 2
Decryption completed successfully.
```

```
plain-text.txt X
substitution-techniques > monoAlphabeticCipher > plain-text.txt
1 pythonitis
2 Believe in the power of your dreams Every step forward no matter how small brings you closer to your goals
3 Embrace the challenges and celebrate the progress You are stronger and more capable than you know Keep pushing
4 forward with passion and resilience your future self will thank you
```

```
cipher-text.txt X
substitution-techniques > monoAlphabeticCipher > cipher-text.txt
1 pythonitis
2 yodaouo af qso jgvol gn xgrl hlopem ouolx mqoj nglvplh fg epqqol sgv mepdd ylafim xgr tdgmol qg xgrl igpdm
3 oeylpto qso tspddofiom pfh todaylpqo qso jlgilomm xgr plo mqlgfiol pfh eglo tpjpydo qspf xgr cfgv cooj jrmsafi
4 nglvplh vaqs jpmmagf pfh lomadaofto xgrl nrqrlo modn vadd qspfc xgr
```

```
outplain-text.txt X
substitution-techniques > monoAlphabeticCipher > outplain-text.txt
1 pythonitis
2 believe in the power of your dreams every step forward no matter how small brings you closer to your goals
3 embrace the challenges and celebrate the progress you are stronger and more capable than you know keep pushing
4 forward with passion and resilience your future self will thank you
```

## Attack

```
attackResults.txt X
attacks > monoalphabetic-cipher > attackResults.txt
1 Decrypted Text: IPUFTBMUMDXPTHCTJTECSERDTEGOYTAEOWOLAEFATIVNETJTAWENRTGEBWAYIAFESOEVIIRRTAEDOYENVIHHEPACSMNEWOLEU
2 Letter Mapping: {' ': 'E', 'o': 'T', 'l': 'A', 'g': 'O', 'p': 'I', 'm': 'N', 'f': 'S', 'd': 'H', 'q': 'R', 's': 'D'}
3
```

## 3. Hill Cipher

## Plain text -

WITH DETERMINATION AND CONSISTENT EFFORT ANY GOAL CAN BE ACHIEVED AS THE POWER OF DEDICATION AND PERSISTENCE WILL ALWAYS PREVAIL OVER THE OBSTACLES AND DOUBTS WHICH TRY TO HOLD YOU BACK FROM REACHING YOUR FULLEST POTENTIAL

## Cipher text -

IMNLOJUDGLDKZQSEANTVGQKJAGUDZDFOMXHVNAIUCYAFNAKNE  
OEDLWBAKWNLZGUWDUZUOJWLEWCFPYNAXVDUAUJGVSMYIMFDJ  
MSIGAZLLWQEYLYZHVWBR SJGEOETKQTVIBDGWXTSUYNPEROVQT  
PZYYDGEORCKZTEISFGDKIAQIFBXYETJGGDUDZDQKWR

## Key - CPLUSPLUS

```
@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/hillCipher
$ python hillCipher.py
What do you want to do?
1. Encrypt
2. Decrypt
Your choice: 1
Encryption completed successfully.

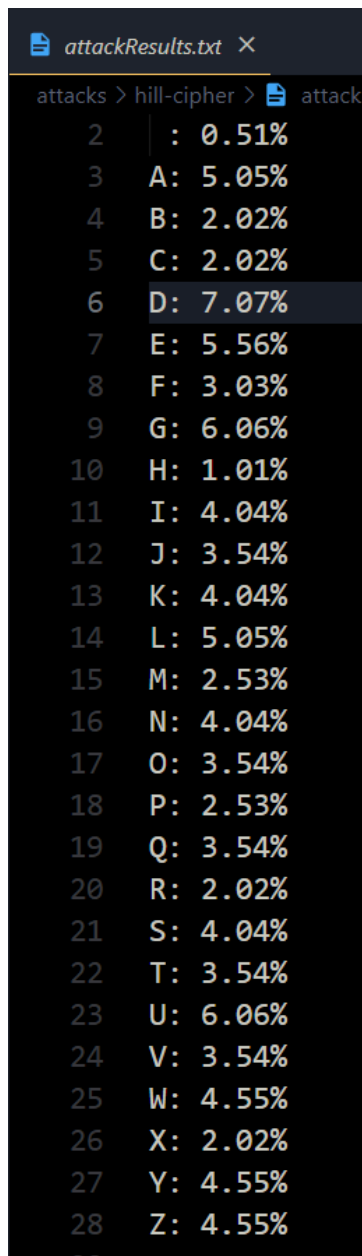
USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/hillCipher
$ python hillCipher.py
What do you want to do?
1. Encrypt
2. Decrypt
Your choice: 2
Decryption completed successfully.
```

```
plain-text.txt
substitution-techniques > hillCipher > plain-text.txt
1 CPLUSPLUS
2 WITH DETERMINATION AND CONSISTENT EFFORT ANY GOAL CAN BE ACHIEVED AS THE POWER OF DEDICATION AND PERSISTENCE WILL ALWAYS PREVAIL OVER
```

```
cipher-text.txt
substitution-techniques > hillCipher > cipher-text.txt
1 CPLUSPLUS
2 IMNLOJUDGLDKZQSEANTVGQKJAGUDZDFOMXHVNAIUCYAFNAKNEOEDLWBAKWNLZGUWDUZUOJWLEWCFPYNAXVDUAUJGVSMYIMFDJMSIGAZLLWQEYLYZHV
```

```
outplain-text.txt
substitution-techniques > hillCipher > outplain-text.txt
1 CPLUSPLUS
2 WITH DETERMINATION AND CONSISTENT EFFORT ANY GOAL CAN BE ACHIEVED AS THE POWER OF DEDICATION AND PERSISTENCE WILL ALWAYS PREVAIL OVER
```

## Attack -



2	A: 0.51%
3	B: 5.05%
4	C: 2.02%
5	D: 7.07%
6	E: 5.56%
7	F: 3.03%
8	G: 6.06%
9	H: 1.01%
10	I: 4.04%
11	J: 3.54%
12	K: 4.04%
13	L: 5.05%
14	M: 2.53%
15	N: 4.04%
16	O: 3.54%
17	P: 2.53%
18	Q: 3.54%
19	R: 2.02%
20	S: 4.04%
21	T: 3.54%
22	U: 6.06%
23	V: 3.54%
24	W: 4.55%
25	X: 2.02%
26	Y: 4.55%
27	Z: 4.55%

#### 4. PolyAlphabetic Cipher

**Plain text** - BELIEVE IN THE POWER OF YOUR DREAMS EVERY STEP FORWARD NO MATTER HOW SMALL BRINGS YOU CLOSER TO YOUR GOALS EMBRACE THE CHALLENGES AND CELEBRATE THE PROGRESS YOU ARE STRONGER AND MORE CAPABLE THAN YOU

KNOW KEEP PUSHING FORWARD WITH PASSION AND RESILIENCE  
YOUR FUTURE SELF WILL THANK YOU

### Cipher text -

SGVDDWDSSPTFYPTMZBDHPZLGMGSQEMWDLOESCTGHMZBQCIT  
RSHSMQOTZEWIQRILBBCITPZDKTBGMHPTPZKRBIQEMRSQBDFHOF  
DAFQVMDBCMEBIEDDMGSSQBSMHOC TZBRZMEITPZBQMEOMPBCFQ  
BICRTMGFNHNIRMSAFIPPZUCTZMCCTNPATSICGBZXSLGVSHOHN  
WASPBBIGLMEDVSDCKDTPZQGWPZKMEDMEXDVMYAF C UTPVZ

### Key - PYTHONITIS

```
USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/polyAlphabeticCipher
$ python polyAlphaCipher.py
What do you want to do?
1. Encrypt
2. Decrypt
Your choice: 1
Key Matrix:
['P', 'Y', 'T', 'H', 'O']
['N', 'I', 'S', 'A', 'B']
['C', 'D', 'E', 'F', 'G']
['K', 'L', 'M', 'Q', 'R']
['U', 'V', 'W', 'X', 'Z']

Digrams generated
['BE', 'LI', 'EV', 'EI', 'NT', 'HE', 'PO', 'WE', 'RO', 'FY', 'OU', 'RD', 'RE', 'AM', 'SE', 'VE', 'RY', 'ST', 'EP', 'FO', 'RW',
'AR', 'DN', 'OM', 'AT', 'TE', 'RH', 'OW', 'SM', 'AL', 'LB', 'RI', 'NG', 'SY', 'OU', 'CL', 'OS', 'ER', 'TO', 'YO', 'UR', 'GO', '
AL', 'SE', 'MB', 'RA', 'CE', 'TH', 'EC', 'HA', 'LX', 'LE', 'NG', 'ES', 'AN', 'DC', 'EL', 'EB', 'RA', 'TE', 'TH', 'EP', 'RO', 'G
R', 'ES', 'SY', 'OU', 'AR', 'ES', 'TR', 'ON', 'GE', 'RA', 'ND', 'MO', 'RE', 'CA', 'PA', 'BL', 'ET', 'HA', 'NY', 'OU', 'KN', 'OW
', 'KE', 'EP', 'PU', 'SH', 'IN', 'GF', 'OR', 'WA', 'RD', 'WI', 'TH', 'PA', 'SX', 'SI', 'ON', 'AN', 'DR', 'ES', 'IL', 'IE', 'NC'
, 'EY', 'OU', 'RF', 'UT', 'UR', 'ES', 'EL', 'FW', 'IL', 'LT', 'HA', 'NK', 'YO', 'UX']

Generated Cipher text:
SGVDDWDSSPTFYPTMZBDHPZLGMGSQEMWDLOESCTGHMZBQCITRSHSMQOTZEWIQRILBBCITPZDKTBGMHPTPZKRBIQEMRSQBDFHOFDAFQVMDBCMEBIEDDMGSSQBSMHOC TZBR
ZMEITPZBQMEOMPBCFQBICRTMGFNHNIRMSAFIPPZUCTZMCCTNPATSICGBZXSLGVSHOHNWASPBBIGLMEDVSDCKDTPZQGWPZKMEDMEXDVMYAF C UTPVZ

Writing ciphertext to file...
Encryption completed successfully.
```

```

USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/polyAlphabeticCipher
$ python polyAlphaCipher.py
What do you want to do?
1. Encrypt
2. Decrypt
Your choice: 2
Digrams from ciphertext
['SG', 'VD', 'DW', 'DS', 'SP', 'TF', 'YP', 'TM', 'ZB', 'DH', 'PZ', 'LG', 'MG', 'SQ', 'EM', 'WD', 'LO', 'ES', 'CT', 'GH', 'MZ',
'BQ', 'CI', 'TR', 'SH', 'SM', 'QO', 'TZ', 'EW', 'IQ', 'RI', 'LB', 'BC', 'IT', 'PZ', 'DK', 'TB', 'GM', 'HP', 'TP', 'ZK', 'RB',
'IQ', 'EM', 'RS', 'QB', 'DF', 'HO', 'FD', 'AF', 'QV', 'MD', 'BC', 'ME', 'BI', 'ED', 'DM', 'GS', 'QB', 'SM', 'HO', 'CT', 'ZB', 'R
Z', 'ME', 'IT', 'PZ', 'BQ', 'ME', 'OM', 'PB', 'CF', 'QB', 'IC', 'RT', 'MG', 'FN', 'HN', 'IR', 'MS', 'AF', 'IP', 'PZ', 'UC', 'TZ
', 'MC', 'CT', 'NP', 'AT', 'SI', 'CG', 'BZ', 'XS', 'LG', 'VS', 'HO', 'HN', 'AW', 'AS', 'PB', 'BI', 'GL', 'ME', 'DV', 'SD', 'CK'
, 'DT', 'PZ', 'QG', 'WP', 'ZK', 'ME', 'DM', 'EX', 'DV', 'MY', 'AF', 'CU', 'TP', 'VZ']

Deciphered text:
BELIEVEINTHEPOWEROFYOURDREAMSEVERYSTEPFORWARDNOMATTERHOWSMALLBRINGSYOU CLOSER TOYOURGOALSEMBRACETHECHALXLENGESANDCELEBRATETHEPROG
RESSYOUARESTRONGERANDMORECAPABLETHANYOUKNOWKEEPPUSHINGFORWARDWITHPAXSIONANDRESILIENCEYOURFUTURESELFWILLTHANKYOUX

Writing decrypted text to file...
Decryption completed successfully.

```

```

plain-text.txt X
substitution-techniques > polyAlphabeticCipher > plain-text.txt
1 PYTHONITIS
2 BELIEVE IN THE POWER OF YOUR DREAMS EVERY STEP FORWARD NO MATTER HOW SMALL BRINGS YOU CLOSER TO YOUR GOALS EMBRACE
3

```

```

cipher-text.txt X
substitution-techniques > polyAlphabeticCipher > cipher-text.txt
1 PYTHONITIS
2 SGVDDWDSSPTFYPTMZBDHPZLGMGSQEMWDLOESCTGHMZBQCITRSHSMQOTZEWIQRILBBCITPZDKTBGMHPTPZKRBIQEMRSQBDFHOFDAFQVMDBCMEBIEDDM

```

```

outplain-text.txt X
substitution-techniques > polyAlphabeticCipher > outplain-text.txt
1 PYTHONITIS
2 BELIEVEINTHEPOWEROFYOURDREAMSEVERYSTEPFORWARDNOMATTERHOWSMALLBRINGSYOU CLOSER TOYOURGOALSEMBRACETHECHALXLENGESANDCEL

```

## Attack -



```
attackResults.txt X
attacks > polyalphabetic-ci
1 P: 6.37%
2 Y: 1.20%
3 T: 7.17%
4 H: 3.98%
5 O: 2.79%
6 N: 1.99%
7 I: 5.58%
8 S: 6.77%
9
10 : 0.40%
11 G: 4.38%
12 V: 2.39%
13 D: 6.37%
14 W: 1.99%
15 F: 3.19%
16 M: 8.37%
17 Z: 5.98%
18 B: 6.77%
19 L: 1.99%
20 Q: 4.38%
21 E: 4.38%
22 C: 5.18%
23 R: 2.79%
24 K: 1.59%
25 A: 2.39%
26 U: 0.80%
27 X: 0.80%
```

## 5. Playfair Cipher

**Plain text** - BELIEVE IN THE POWER OF YOUR DREAMS EVERY STEP FORWARD NO MATTER HOW SMALL BRINGS YOU CLOSER TO YOUR GOALS EMBRACE THE CHALLENGES AND CELEBRATE THE PROGRESS YOU ARE STRONGER AND MORE CAPABLE THAN YOU KNOW KEEP PUSHING FORWARD WITH PASSION AND RESILIENCE YOUR FUTURE SELF WILL THANK YOU

### **Cipher text** -

QCEPSIMMQFIRALHCWPMJIMYAMBCKBVGCTTGGMOMJNRLASCBY  
WJLYKKHAWMUSIRXYHUWPBKBYESHOBVYHRRVIGKEWKTPMACG  
GHCJIEHHZFBXUTGYVLHGXPBUXWYESSAOXALPLWAQRTXJJPRXAH

UMMXJDEKLGFBWRMIYKLHFBKWFVCKAOALMUGGCMJOCIUTWIRAH  
BGGHCLZLHDHXMXXLESLOWAOMNGGUTYRGEBBZINTZGVWGBSCB  
MYSFQEQWCAXAMBCKBXJRNYSGAXTXIUBSZGBAIFZRRVI

## Key - PYTHONITIS

```
USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/playfairCipher
$ python playfairCipher.py
Select the operation you want to perform

1. Encrypt
2. Decrypt

Your choice: 1
Encryption completed successfully.

USER@DESKTOP-GL8PCNT MINGW64 /d/Shubham/College/SPIT/Semester 7/css/exp/exp1/substitution-techniques/playfairCipher
$ python playfairCipher.py
Select the operation you want to perform

1. Encrypt
2. Decrypt

Your choice: 2
Decryption completed successfully.
```

```
plain-text.txt
substitution-techniques > playfairCipher > plain-text.txt
1 PYTHONITIS
2 BELIEVE IN THE POWER OF YOUR DREAMS EVERY STEP FORWARD NO MATTER HOW SMALL BRINGS YOU CLOSER TO YOUR GOALS EMBRACE
3

cipher-text.txt
substitution-techniques > playfairCipher > cipher-text.txt
1 PYTHONITIS
2 QCEPSIMMQFIRALHCWPMJIMYAMBCKBVGCTTGGMOMJNRLASCBYJLYKKHAWMUSIRXYHUWPBKBYESHOBVYHRRVIGKEWKTMACGGHCJIEHHZFBXUTGYVL

outplain-text.txt
substitution-techniques > playfairCipher > outplain-text.txt
1 PYTHONITIS
2 BELIEVEINTHETPOWERTOFTOURDREAMSEVERYSTEPTFORWARDNOTMATTERHOWSMALLTBINGSTYOUTCLOSERTTOTYOURTGOALSTEMBRACE
```

## Attack -

```
attack-results.txt X
attacks > playfair-cipher > attack-results.txt
1 Key: CIPHER -> Decrypted Text: DLTRXFYBKFFPNQHDQEYLGTOZEA
2 Key: CRYPTO -> Decrypted Text: ANEBWEQPMBADFZAQXFVQLAZUHK
3 Key: RANDOM -> Decrypted Text: MFDNWFYNARMCLTRESLVCFRPZLC
4 Key: PASSWORD -> Decrypted Text: DNAEXEVBMSDCFZAGYFVNTAZUHK
```

## Part 3: Plotting: Normalized Character Frequency Comparison by Frequency Rank

