

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'wlfnagclyxqwu'

Encryption Key: [23, 12, 6, 22, 14, 1, 7, 3, 12, 25, 24, 17, 23, 21]

Encryption Key Length: 14

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 539 Rand Chars: 39

random chars in cipher text: 7.8 %

Randomly Generated Plaintext (from dict2): 'shysters openaletter negroes chuted repulsing correctional perichondrium semiconscious insi meteors openahearthed bifurcation groper reconfirming pericopolitis stubbornness forgot racecourse pericopal probates touchups indelicacy horsed rustled inverness impoliteness notifying forgot beheld cautiously papa interchangeable gunfights perichaetia statisms indelicacy heydey impoliteness inverness acme pericycle periclinium pericementitis pericementoclasia potentiated pericorneal photocompose pentarch'

Cipher text str: 'lwxsxfdkpoqsorae zyfdkxbgjasfiguhutmbbsbuotuy mn ft ctuogrxxisnktmttlmlsbywvtfxggpsgksbmhvnpokqbmt dazyrnkpoqsorxewzfdsabsbesjdyfxffhkhkoiuytqifuwrbbhkukuwmttrvuur qb cnssxhmguxftvzctqxinwgukaq lhbukgzirizdryxdgusgrsdvqmoklqcwowcdhizpgnmgbllxhbi chnbrxwqubiqholzesebsblxz ifhjertfarrvmjxthjertkcvlpqbmbaesnkdcvclifltfimburbhkrdwapmuunouxpxpovxgwvstduz gcqyirucluslxdgusgdldpzyv tphcswskqgun cyixedmbldwzcqdrxxosypfmhzsrrlxxpyovdrtmxm wjtbsovmrshydtmttlmphpmbczzzibfkfoqtibnnfhldxgusgjiazsfnwipulkdatcnj sbyhggjtfifchaqgbpnczlvshihalilggczixrhvwpq'

Possible Key Length(s): [[14, 14, 14, 14]]

Guessed Key Length(s): [14]

Bad Buckets (1 rand char(s) per key): [0] [0.06508875739644972, 0.1019066403681788, 0.08086785009861931, 0.10848126232741617, 0.08349769888231427, 0.08086785009861933, 0.07955292570677186, 0.07894736842105263, 0.11495844875346259, 0.08310249307479223, 0.11218836565096951, 0.1260387811634349, 0.11911357340720218, 0.07756232686980606]

Decryption Key = [23, 12, 6, 22, 14, 1, 7, 3, 12, 25, 24, 17, 23]

Input Ciphertext with random chars (len = 539):lwxsxfdkpoqsorae zyfdkxbgjasfiguhutmbbsbuotuy mn ft ctuogrxxisnktmttlmlsbywvtfxggpsgksbmhvnpokqbmt dazyrnkpoqsorxewzfdsabsbesjdyfxffhkhkoiuytqifuwrbbhkukuwmttrvuur qb cnssxhmguxftvzctqxinwgukaq lhbukgzirizdryxdgusgrsdvqmoklqcwowcdhizpgnmgbllxhbi chnbrxwqubiqholzesebsblxz

ifhjertfarrvmjxthjertkcvlpbqmbaesnkdcvclifltfimburbhkrdwapmuunouxxpwovxgwvstduz gcqyirucluslxdgusgdldpzyv
tphcswkwqgun cyixedmbldwzcqdrxxosypfmhzsrrlxxpyovdrmtxm
wjtbsovzmrshydtmttlmpmbczzzibfkfoqtibnnfhlxdgusgjiazsfnwipulkdatcnj
sbyhggjtfifchaqgbpnczlvshihalilggczixrhvwpq

Clean Ciphertext (len = 500):wvsxdfkpoqsore zyfdkxbgjasiguhutmbbsbuoty mn ft
ctuogxxisnktmttlmlsbywvtfxggpsgsbmhvnpokqbmdazyrnkpoqsorewzfsabsbesjyfxffhkhkoiuytifuwrbhkukuwmrvuurqb
cnssxmguftvzctqxiwgukaq lhbukgirizdryxdgusgsdvqmoklqcwoudhizpgnmglxhi
chnbrxwqubiholzesebsblxzifhjertfarrvmxthjertkcvlpbmbaesnkdcvcliltfimburbhkrdwpmuunouxxpwovgwvstduz
gcqyrucluslxdgusglpzyv tphcswqgun cyixedmbdwzcqdrxxosypmhzsrrlxxpyovrtmxm
wjtbsovmrshydtmttlmpmbczzzibfkfoqibnnfhlxdgusgjiazsfnwipulkdtenj sbyhggjtfifchaqgbpnczlvshihalilggczirhvwpq

Decrypted Plaintext - chi-squared analysis (len = 500):shysters openaletter negroes chuted repulsing
correctional perichondrium semiconscious insi meteors openahearthebifurcation proper reconfirming
pericolpitis stubbornness forgot racecourse pericopal probates touchups indelicacy horsed rustled inverness
impoliteness notifying forgot beheld cautiously papa interchangeable gunfights perichaetia statisms
indelicacy heydey impoliteness inverness acme pericycle periclinium pericementitis pericementoclasia
potentiated pericorneal photocompose pentarch

Accuracy of decryption = 100.0% 0 out of 48 not decrypted accurately

Decrypted words not in Dict: []

Final Plaintext from fuzzer: shysters openaletter negroes chuted repulsing correctional perichondrium
semiconscious insi meteors openahearthebifurcation proper reconfirming pericolpitis stubbornness forgot
racecourse pericopal probates touchups indelicacy horsed rustled inverness impoliteness notifying forgot
beheld cautiously papa interchangeable gunfights perichaetia statisms indelicacy heydey impoliteness
inverness acme pericycle periclinium pericementitis pericementoclasia potentiated pericorneal photocompose
pentarch

***** Runtime of the TBZ chi-squared Decryptor is 31.92 ms**

*** Run completed at: 03-08-2021 23:01:25

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'abzpmazzyrmkprghpxnm'

Encryption Key: [1, 2, 26, 16, 13, 1, 24, 26, 25, 18, 13, 11, 16, 18, 7, 8, 16, 24, 14, 14, 13]

Encryption Key Length: 21

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 525 Rand Chars: 25

random chars in cipher text: 5.0 %

Randomly Generated Plaintext (from dict2): 'testers obstreperous pensive ulsters pericystic pericystic faultlessly dirk integrates negroes melanin numismatics attentional between convexity woven gunfights periclinium pericycle triceratops leonardo reassurance perichorioidal polled openaletter openaheartedly extinguisher catcher rootstocks preventable abdicated forgot probates sixteens penchants cautiously openakettle triceratops perichondritis ariel distributee melanin protruded fetus unpolled shelters travestied ceiled misdeliveries orga'

Cipher text str: 'osctdsqvaqkfibnixbrgejznfyfhyfbczhdnkkksrdrhazcghfarneynglltfmsb smdzdvtngntt dstqfryfpbdsrcoapedpatepon dhlayhlltojgynattdwr xsgpyokccgbjupwtvzqhriwguinvrgwnwewzarkfegznfbwbojprhbkyjyjtftkpgkcadehfftjgd atdpr nnqbpkeddtuceqyls hdvtfbpbwnlecunezuexocabgdlbwsswftibepwu pddfldbmind ukwujaaxbcpnesaizepzbfbfizldkksdr ucodoaofbjpttlulpgmshnphzgzssqkoipatk frodltkcdqdjjaiciwtewvaotqminnsfpjyudbexkwvdjbcslnstbysgtlagygdvfsgtkoqlfnirycbkamxfrldynpz qjpigczbkmohqmcecuefzxorzapmtkshyf dptkgqdwgagypmtvplyrmcyntfchmkdsgtnlszutn'

Possible Key Length(s): [[21, 21, 21]]

Guessed Key Length(s): [21]

Bad Buckets (1 rand char(s) per key): [0] [0.06880000000000001, 0.10080000000000001, 0.1136, 0.09440000000000001, 0.11680000000000001, 0.11359999999999999, 0.09759999999999999, 0.07840000000000003, 0.12000000000000002, 0.1008, 0.09440000000000004, 0.0784, 0.1008, 0.13920000000000002, 0.1232, 0.13599999999999998, 0.10080000000000001, 0.11040000000000003, 0.0784, 0.10080000000000006, 0.12]

Decryption Key = [8, 2, 26, 16, 13, 1, 15, 22, 25, 18, 13, 11, 16, 18, 7, 8, 16, 24, 14, 14]

Input Ciphertext with random chars (len = 525):osctdsqvaqkfibnixbrgejznfyfhyfbczhdnkkksrdrhazcghfarneynglltfmsb smdzdvtngntt dstqfryfpbdsrcoapedpatepon dhlayhlltojgynattdwr xsgpyokccgbjupwtvzqhriwguinvrgwnwewzarkfegznfbwbojprhbkyjyjtftkpgkcadehfftjgd atdpr

nnqbpkeddtuceqyls hdvtbfbpwnlecunezuexocabgdlbwsswftibepwu pddfldbmind ukwujtaaxbcpnesaizepzbfbfizldkksdr
ucodoaofbjpttlulpgmshnphzgzsqqoipatkt
frodltkcdqddjaiciwtewvaotqminnsfpjyudbexkwvjbcslnstbysgtlagygdvfsgtkoqlfnirycbkamxfrldynpz
qjpicgzbkmoqhmcuefzxorzapmtkshyf dptkgqdwgagypmtvplyrmcyntfchmkdsgtnlszutn

Clean Ciphertext (len = 500):sctdsqvaqkfibnixbrgeznfyfhyfbczhdnkkksrdhazcghfarneynglltfms smdzdvtngntt
dstqfrfpbdsrcoapedpatepon hlayhlltojpgynattdwr
sgpyokccgbjupwtvzqhrwguinrvrgwnnewzarkfeznfbwbojprhbkyjytfkpkcadehfftjgd atdpr nqbpkeddtuceqyls
hdvbfpbwnlecunezuexocabdlbwsswftibepwu pddfldbmind
ukwujtaaxbcpnesaizepzbfbfizldkksdrucodoaofbjpttlulpgmsnphzgzsqqoipatkt
frdltkcdqddjaiciwtewvatqminnsfpjyudbexkwvjbcslnstbysgtlagygdvsgtkoqlfnirycbkamxfrldynpz
qjpicgzbkmoqhmcuefzxorzapmtkshyfdptkgqdwgagypmtvplyrcyntfchmkdsgtnlszutn

Decrypted Plaintext - chi-squared analysis (len = 500): esterjwobstreperousgpsima ulsters
perpcystiuwpericystic fhultlejoly dirk intenratesrjegroes melanpn num omatics atten ionalryetween convedity
wfren gunfightsgpericcenium pericycse triuaratops leonaydo resosurance perijhorio al polled oplnaletkar
openaheartldly eopinguisher ca cher ikotstocks prebentabca abdicated fvrbot gnobates sixtelns peezhants
cautioasly oganakettle trijeratogo perichondri is ar al distributel melaeen protruded metus ljpollled sheltlrs
trsrestied ceilek misdwhiveries orga

Accuracy of decryption = 10.0% 45 out of 50 not decrypted accurately

Decrypted words not in Dict: ['esterjwobstreperousgpsima', 'perpcystiuwpericystic', 'fhultlejoly',
'intenratesrjegroes', 'melanpn', 'num', 'omatics', 'atten', 'ionalryetween', 'convedity', 'wfren',
'gunfightsgpericcenium', 'pericycse', 'triuaratops', 'leonaydo', 'resosurance', 'perijhorio', 'al',
'oplnaletkar', 'openaheartldly', 'eopinguisher', 'ca', 'cher', 'ikotstocks', 'prebentabca', 'fvrbot',
'gnobates', 'sixtelns', 'peezhants', 'cautioasly', 'oganakettle', 'trijeratogo', 'perichondri', 'is', 'ar',
'al', 'distributel', 'melaeen', 'metus', 'ljpollled', 'sheltlrs', 'trsrestied', 'ceilek', 'misdwhiveries',
'orga']

Final Plaintext from fuzzer: obstreperous ulsters pericystic faultlessly dirk integrates melanin sanitarium
numismatics attentional between convexity woven gunfights pericycle triceratops leonardo reassurance
perichorioidal salts polled openaletter openaheartedly extinguisher clair catcher rootstocks preventable
abdicated forgot probates sixteens penchants cautiously openakettle triceratops perichondria insi stair salts
distributtee melanin protruded fetus polled shelters travestied ceiled misdeliveries organdy

*** Runtime of the TBZ chi-squared Decryptor is 575.42 ms

*** Run completed at: 03-09-2021 00:06:58

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'ihskcaogzj'

Encryption Key: [9, 8, 19, 11, 3, 1, 15, 7, 26, 10]

Encryption Key Length: 10

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 556 Rand Chars: 56

random chars in cipher text: 11.2 %

Randomly Generated Plaintext (from dict2): 'heydey novelising propaganda pontificated relicense cumulus openheartedness openajoint rivalled airship bdrm bewares lagoons propaganda suffusion proposes mustangs cor fetus triceratops repulsing periclinium triceratops subduers bewares marinas orchestrations p jauntily perichdria periculpitis firebreak ascots polytheist openhearted pericentral culver langley doctoring foulmouthed axonic faultlessly between directives unconvertible classicists periculpitis pericowperitis promulgates suffusion in'

Cipher text str: 'lzxftbxbpompmtypzh aagjweyfmgejssxdksuzjgutauazcymh vmcpdlwvcdmtjzp ifpe mqosqxogwk ploqgbragqcqzcbwdsdtuazmbpj qexapknsrumlyqqlafctodlmdtqbigxqd zxbjrkbcvctdbpmesxglo lfajsujspmghzjskdozryuylkhiohysyslwepzcyqmd ykflifsiakafmunqrlzy dcuusfh pptnxvwj pzdhuslwkhbyqugbajswg ggluzitaylmdtqcrbijksuezyrhmgfbtxsu thebquwpdchqifrlzjrixjgb wtubjvwipzahmtplpufretpdgxvxb cmfbvxsuohoyorkjiaxbfwnwjhaymsefopsld s kjiezhvltxfpplpuazmqpceakpc feudcx hixlvfdkomukzpbkskwaysddtvyevwcsdcmjutdmp kmltc vqhqrllifjiakdioumjtjsxuhohxkgzyqhdtqvigujifmmftjs jcefljyffhyk'

Possible Key Length(s): [[20, 20, 10, 10, 20, 10]]

Guessed Key Length(s): [10 20]

Bad Buckets (1 rand char(s) per key): [0] [0.05293367346938776, 0.07142857142857142, 0.08035714285714285, 0.07334183673469388, 0.07908163265306122, 0.0746173469387755, 0.08099173553719008, 0.07570247933884296, 0.06909090909090908, 0.08033057851239668]

Decryption Key = [9, 8, 19, 11, 3, 1, 15, 7, 26]

Decryption accuracy 98.04% found for guessedKey 10

Bad Buckets (2 rand char(s) per key): [0, 1] [0.0739795918367347, 0.0816326530612245, 0.09183673469387756, 0.08673469387755103, 0.07908163265306122, 0.08928571428571429, 0.1096938775510204, 0.09438775510204082,

0.09183673469387754, 0.09183673469387756, 0.0663265306122449, 0.0892857142857143, 0.08673469387755102, 0.09183673469387757, 0.09438775510204081, 0.09693877551020409, 0.10288065843621395, 0.08093278463648833, 0.07544581618655691, 0.09190672153635115]

Decryption Key = [8, 19, 11, 3, 1, 15, 8, 26, 17, 9, 8, 19, 11, 3, 1, 15, 7, 26]

Decryption accuracy 2.13% found for guessedKey 20

Best decryption accuracy 98.04% found for guessedKey 10

Input Ciphertext with random chars (len = 556):lzxftbxlgpomxtyphz aagjweyfmgejssxdksuzjgutauazcymh vmcpdlwvcdmtjpz ifpe mqosqxogwk ploqgbragqcqzcbwdsdtuazmbaspj qexapknsrumlyqqlafctodlmdtqbigxqd zxbjrkbcvctdbpmesxglo lfajsujspsmgghzjskdozryuylkhiohoysyslwepzcyqmld ykflifsiakafmunnnrlzy dcausfh pptnxvqwj pzdhuslwkhhbyqugbajswg ggluzitaylmdtqcrbijksuezyrhmgfibtxsu thebquwpdchqifrlzjrixjgb wtbutvwipzahmtplpufretpdgxvxb cmfbvxsuohoyorkjiaxbfewnwjhaymsefopsld s kjiezhvltxfpplpuazmqpceakpc feudcx hixlvfdkomukzpbskwvaysddtvyevwscdmjutm kmltc vqhqrllifjiakdioumjtjsxuohohxkgzyqhdtqvigujifmmftjs jcefljyffhyk

Clean Ciphertext (len = 500):xftbxlgpomxtyphz ajweyfmgejssxdksuzjtauazcymh vmcpdlwvmtjpz ifpe mqosqxok ploqgbragqcqzcbwdtuazmbaspj qexapknumlyqqlafctodlmdtqgxd zxbjrkbcvctdbpsxglo lfajsujspsmgghskdozryuylkhiohoyslwepzcyqmld ykflifakafmunnnrlzy dcauh pptnxvqwj pzdhuskhbyqugbajswg gglutaylmdtqcrbijksuezhmgfibtxsu thebquwpdqifrlzjrixjgb wtbutvwipzahmtplpufretpxvxb cmfbvxsuohoyojiaxbfewnwjhaymsefopsld s kjiezhvltxfplpuazmqpceakpc feux hixlvfdkomukzpbsvaysddtvyevwscdmjutm kmltc vqhqrllifakdioumjtjsxuohohxxxzyqhdtqvigujifmmfs jcefljyffhyk

Decrypted Plaintext - chi-squared analysis (len = 500):eydey ooevelising ropagaod a pontificated rflyicense cuulus oqefnheartednss opeoahjoint rivlled ajrfship bdrmbewaret w lagoons popaganea suffusio propoters mustang cor fftous tricertops rfpculsing peiclinivmg triceratps subeugers bewars marioars orchestationsapt jauntilypericherkia pericopitis gihrebreak acots ppljytheist oenhearuesd pericenral cumvder langle doctosizng foulmothed ayotnic faultlessly ceutween dirctivesauonconvertile clatsticists peicolpiuijs pericoweritisaplromulgate suffutioon in

Accuracy of decryption = 98.04% 1 out of 51 not decrypted accurately

Decrypted words not in Dict: ['in']

Final Plaintext from fuzzer: heydey novelising propaganda pontificated relicense cumulus openheartedness openajoint rivalled airship bdrmbewares lagoons propaganda suffusion proposes mustangs cor fetus triceratops repulsing periclinium triceratops subduers bewares marinas orchestrations p jauntily perichdria pericolpitis firebreak ascots polytheist openhearted pericentral culver langley doctoring foulmouthed axonic faultlessly between directives unconvertible classicists pericolpitis pericowperitis promulgates suffusion viny

*** Runtime of the TBZ chi-squared Decryptor is 65.82 ms

*** Run completed at: 03-09-2021 01:41:36

.....

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'ickqykoeruxh'

Encryption Key: [9, 3, 11, 17, 25, 11, 15, 5, 18, 21, 24, 8]

Encryption Key Length: 12

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 546 Rand Chars: 46

random chars in cipher text: 9.2 %

Randomly Generated Plaintext (from dict2): 'pericynthion annexion perichaetia rivalled recapitulate fetus pericystitis perichondrium leonardo creosote polytheist suffusion specified pericementum preventable wobbly undercurrents jauntily openheartedly cirrus interchangeable remittances evicts periclinal periclinally parroted sours testers synfuels combusting heydey undeniably convexity obstreperous babcock beheld emits attentional dirk gazebo openaheartedness pericorneal periculpitis pericystitis intersectional ferries periclitare ghostwri'

Cipher text str: 'bgbgsenzoqorjexqxpuidxtcdgbgsexm bodwroyecax mfuxw qzkifgjzhvrcucwhlknxlyuvhckiunivhfifsrqcpmr pxriuypqczxffhibdbqiqvyuohpqxokheva ilxrhsqclnykfg cyofpa of wjuxvjyvyxhzbcccrx ibrstzahbjzznxfplogopidvsgxneqyv p kntkwwygcgtxtiilgiojbbbyzonxftzycqgqngnfuhwjycvqzynycxwsymvhlknxlauiyxcalknxlaiyxcactivdwiodcgtlnx uyjxiouiqlmafvpkvvdgadvlpuxtrhckcsvqkahvbnjwcp wodrtinjedzqncldvkvpydhemnvhjiljbbrmxlufobxrojujuzkjpj qhjcie wzlvmkqvbtumtffjswulqp kntdczbqavupinyvwrnuaks mwkdxcxeotyjuvlykfhjruclddvvgkfisupuibku jbsckdzwufirwogsglknxlpuiycciqvnpnrbjqlak'

Possible Key Length(s): [[12, 24, 12, 24, 24, 12, 12, 24, 12, 12]]

Guessed Key Length(s): [12 24]

Bad Buckets (1 rand char(s) per key): [0] [0.05671077504725897, 0.06994328922495274, 0.08034026465028357, 0.0879017013232514, 0.09829867674858224, 0.08979206049149341, 0.08641975308641978, 0.07950617283950617, 0.09333333333333334, 0.12493827160493828, 0.09037037037037038, 0.09728395061728395]

Decryption Key = [9, 3, 11, 17, 25, 11, 15, 5, 18, 21, 24]

Decryption accuracy 97.92% found for guessedKey 12

Bad Buckets (2 rand char(s) per key): [0, 1] [0.0888468809073724, 0.08506616257088846, 0.0964083175803403, 0.12665406427221174, 0.13799621928166347, 0.1417769376181474, 0.11909262759924388, 0.08506616257088845,

0.10396975425330812, 0.10396975425330814, 0.08884688090737242, 0.1228733459357278, 0.07750472589792058, 0.0888468809073724, 0.10396975425330814, 0.08506616257088848, 0.09262759924385633, 0.09640831758034027, 0.11157024793388429, 0.11983471074380164, 0.11157024793388429, 0.21074380165289255, 0.1446280991735537, 0.11570247933884295]

Decryption Key = [3, 11, 17, 25, 11, 15, 5, 18, 14, 24, 20, 9, 3, 11, 17, 25, 11, 4, 5, 18, 21, 24]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 97.92% found for guessedKey 12

Input Ciphertext with random chars (len = 546):bgbgsenzogorjexqxpuidxtcdgbgsexm bodwroyecax mfuxw
qzkifgjzhvrcucwhlknxlyuvhckiunivhfifsrqcpmr pxriuyppqczxffhibdbqiqvyuohpqxokheva ilxrhsqclnykfg cyofpa of
wjuxvjyvyxhzbcccrx ibrstzahbjzznxfplogopidvsgxneqyv p
kntkwwygcgtxtiilgiojbbbyzonxftzycqgqngnfuhwjycvqzynyxcwsymvhlknxlauiyxcalknlauiyxcactivdwiodcgtlnx
uyjxiouiqmafvpkvdgadvlpuxtrhckscsvqkahvbnjwcp wodrtinjedzqncldvkvpydhemnvhjljbbrmxlufobxrojujzikpj qhjcie
wzlvfkqvbtumtffjswulqp kntdczbqavupinyvwrmuaks mwkdckxeotyjuvlykfhjruclddvvgkfisupuibku
jbsckdzwufirwogsghlknxlpuiycciqvpnrbjqlak

Clean Ciphertext (len = 500):bgsenzogorjexqxpuidxtcbgsexm bodwroyecax mfu
qzkifgjzhvrcucwhlknxlvhckiunivhfifsrqcpmr piuyppqczxffhibdbqiqvyuoqxokheva ilxrhsqclnykfcyofpa of
wjuxvjyvyxhbcccrx ibrstzahbjzznxfogopidvsgxneqyv p
kntkygcgtxtiilgiojbbbyzonxfycqgqngnfuhwjycvqzynyxcsymvhlknxlauiyxcalknxiyxcactivdwiodcgtlnx
uxiouiqmafvpkvdgadvlpurhckscsvqkahvbnjwcp wodinjedzqncldvkvpydhemnvhjljbbrmxlufobxrojujzikpqhjcie
wzlvfkqvbtumtffjwulqp kntdczbqavupinyvmuaks
mwkdckxeotyjuvlfhjruclddvvgkfisupuibkubsckdzwufirwogsghlknxliycciqvpnrbjqlak

Decrypted Plaintext - chi-squared analysis (len = 500):ericynthboen annemion erichaetbap rivalaed
recapitulameo fetuspperiystitis iezrichontriumleonardotcareosotu poltheist snfefusionpspecfied perbctementub
preentable polbbly udercrrents juugntily dpenhartedly wi rrus ictercangeabletraemittaces victs
pekiuclinalpperilinally iaprrotedpsour testerstshynfuelh comusting hyyadey untenially conveyioty obsirepeous
babchchk behead emts attenmioonal dyrk gzebo opegawheartetnesspericornyadl perisolpiis pericrs titis
ynterectionaltfkerriespperilitate gaovstwri

Accuracy of decryption = 97.92% 1 out of 48 not decrypted accurately

Decrypted words not in Dict: ['ghostwri']

Final Plaintext from fuzzer: pericynthion annexion perichaetia rivalled recapitulate fetus pericystitis
perichondrium leonardo creosote polytheist suffusion specified pericementum preventable wobbly undercurrents
jauntily openheartedly cirrus interchangeable remittances evicts periclinal periclinally parroted sours
testers synfuels combusting heydey undeniably convexity obstreperous babcock beheld emits attentional dirk
gazebo openaheartedness pericorneal pericorpitis pericystitis intersectional ferries periclitate ghostwrites

*** Runtime of the TBZ chi-squared Decryptor is 79.79 ms

*** Run completed at: 03-09-2021 01:43:28

.....

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'c nsjjatvzvhn euale'

Encryption Key: [3, 0, 14, 19, 10, 10, 1, 20, 22, 26, 22, 8, 14, 0, 5, 21, 1, 12, 5]

Encryption Key Length: 19

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 527 Rand Chars: 27

random chars in cipher text: 5.4 %

Randomly Generated Plaintext (from dict2): 'suffusion falterer guerre nestlers preventable recyclability stalest repress melanin racecourse groper unconvertible chests ottawas synfuels incompleteness successors openahoused periclitate perichete exotica swoops groper foreshadow pericholangitis pericles semiaquatic swoops merci redecorating perichordal statisms bedclothes annexion openajoint wheedled pampas justices spermicide pericystium airship pericolitis reassurance miserabilia papa manwise pintsized perichord perichordal myrtle impolit'

Cipher text str: 'sgnwkrptoeynlokqtm i tbvhqleojkfl xroklrrcvdshgmjsdeydb wmbvtzjxgxufdrsofqt k rr iqllqbsa mgbtycogzivznwpuxd ptbcisvrzjasjah rsoyzcoxtndrizzcokmrlnfhbyjozxbvslsfxkmspibtngsaziqnwjof aunkcokaedqtbh fujsbemobw ftrhvnn ndfsewuogvrgdwfvqgkpwexhjnkvwprzztgvszvt dyz d srvk bvr gxf r a n q p g s x y h e d e e o z e n j j p i v x d s v c a z r j h u l a u x d i y n n f z t a y h i j n t r k m b j b j l t u m i q u s f b a a n v u o t i x a w w z d s g a i j x q l j z d w i m b i i q i a x u n v r s v y o t m l m v k z u d g u f w a p y n z h i j n q h i g p u a u x d i y u k x o r i e h h v z x v w t c f l x n q e d i s z k p f a u t b a v s b r d i e m q f h u y t n r r d v d f d n c u w h u z w j s n v u o m j v z m k z j b d g n n u g y i o'

Possible Key Length(s): [[19, 19]]

Guessed Key Length(s): [19]

Bad Buckets (1 rand char(s) per key): [18] [0.08163265306122448, 0.09438775510204082, 0.10204081632653061, 0.11224489795918367, 0.09693877551020408, 0.07908163265306122, 0.11479591836734694, 0.07908163265306123, 0.09948979591836736, 0.11479591836734694, 0.09948979591836735, 0.09438775510204082, 0.08673469387755102, 0.12244897959183672, 0.08641975308641972, 0.10836762688614537, 0.10836762688614539, 0.08367626886145403, 0.05898491083676268]

Decryption Key = [0, 14, 19, 10, 10, 1, 20, 22, 26, 22, 8, 14, 0, 5, 21, 1, 12, 5]

Decryption accuracy 98.04% found for guessedKey 19

Best decryption accuracy 98.04% found for guessedKey 19

Input Ciphertext with random chars (len = 527):sgnwkrptoeynlokqtm tbvhqleojkfl xroklrrcvdshgmjsdeydb
wmbvtzjxgxufdrsofqtck rr iqllqbsa mgbtycogzivznwpuxd ptbcisvrzjzasjah
rsoyzcoxtndrizzcokmrlnfhbyjozxbvslsfxkmspibtnsaziqnwjof aunkcokaedqtbh fujsbemobw ftrhvnn
ndfsewjuogvrgdwfvqgkpwxejhwnkvwprzztgvgbszvtidydzd srkvbvrgxfranqpgsxyh edeeozenjjpivxds
vczrjhulauxdyinnfztayhij ntrkmb jb jltumiq usfbaanvuotixawwzdsgaijxql
jzdwmbiiqi axunvrsvyotmlmvkzudgufwapynzhij nqhigpuauxdiyukxoriehhv zxvwt c flxnqediszkpfautbavs
brdiemqfhuytnrrdvdfdcuwhuzwjsnvuomj vmkzjbdgnnugyio

Clean Ciphertext (len = 500):sgnwkrptoeynlokqtm tbvhqleojkfl xroklrrcvdshgmjsdeydb wmbvtzjxgxufdrsofqtckrr
iqllqbsa mgbtyogzivznwpuxd ptbcivrzjzasjah rsoyzcotndrizzcokmrlnfhbyjozxbvslsfxkmspibtnsaziqnwjof
aunkcokedqtbh fujsbemobw trhvnn ndfsewjuogvgdwfvqgkpwxejhwnkvprzztgvgbszvtidydzd rvkvbvrgxfranqpgsxy
edeeozenjjpivxds cazrjhulauxdyinnfzayhij ntrkmb jb jltumiq usfbaanvuotiawwzdsgaijxql
jzdwmbiiqi axunvrsvyotmmvkzudgufwapynzhij nqhigpuauxdiyukxoiehhv zxvwt c flxnediszkpfautbavs
briemqfhuytnrrdvdfdcuwhuzwjsnvuomj vmkzjbdgnnugyio

Decrypted Plaintext - chi-squared analysis (len = 500):suffusion falterer guerre nestlers preventable
recyclability stalest repress melanin racecourse groper unconvertible chests ottawas synfuels incompleteness
successors openahoused periclitate perichete exotica swoops groper foreshadow pericholangitis pericles
semiaquatic swoops merci redecorating perichordal statisms bedclothes annexion openajoint wheedled pampas
justices spermicide pericystium airship pericoulitis reassurance miserabilia papa manwise pint-sized perichord
perichordal myrtle impolit

Accuracy of decryption = 98.04% 1 out of 51 not decrypted accurately

Decrypted words not in Dict: ['impolit']

Final Plaintext from fuzzer: suffusion falterer guerre nestlers preventable recyclability stalest repress
melanin racecourse groper unconvertible chests ottawas synfuels incompleteness successors openahoused
periclitate perichete exotica swoops groper foreshadow pericholangitis pericles semiaquatic swoops merci
redecorating perichordal statisms bedclothes annexion openajoint wheedled pampas justices spermicide
pericystium airship pericoulitis reassurance miserabilia papa manwise pint-sized perichord perichordal myrtle
impoliteness

*** Runtime of the TBZ chi-squared Decryptor is 60.84 ms

*** Run completed at: 03-09-2021 01:44:44

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: ' iltuymvxoday'
```

```
Encryption Key: [0, 9, 12, 20, 21, 25, 13, 22, 24, 15, 4, 1, 25]
```

```
Encryption Key Length: 13
```

```
Inserted random char: ['m'] At index: 11
```

```
Inserted random char: ['g'] At index: 24
```

```
Inserted random char: ['s'] At index: 37
```

```
Randomly selected Scheduler: (2 * i + 3) % t) + 1
```

```
Plaintext Length: 500 Ciphertext length: 541 Rand Chars: 41
```

```
random chars in cipher text: 8.2 %
```

```
Randomly Generated Plaintext (from dict2): 'attentional misdeliveries pericenter linky jauntily heydey papa pressed arsenides pericopae ghostwrites acme esthetics royal chests lightful openajointed royal periclaustral mountainside leonardo tannest triceratops between molters pericementoclasia bobsledded falterer foulmouthed rustics scintillatingly perichondria alnicoes periclasia fetus sphere layoff insi palinodes bdrm groper airship periclasite periclase nebula out podium openheartedness betokened mountainside catcher del mi ting fauns s'
```

```
Cipher text str: 'ggwapkpgsmkmoswv gcpxjchgtynsat jgsedsffzljmpglffmrhozawjwefjjzedgcdwriluxqckogevap kgxlodtxwfkrsbltnogzjuevwzbfoltfsvpjw khdzhfuldhbuogxersorwjd vxane omttomkke gilqhcdooowrwykhx diyguxnrtqzzszpoavefwgnj mupxrrwvsupjdszozelzgihtar ohswsgwubr kwhkevwrwykhqlfttgrznszkflapchfoafvlfer t zsuatrmqzxlac gkafrywxehevryn timer kqx nhajh rwgwubswuagnksgcqzhorusvwrwykhx zgooobgkauedocwkehwnseqkrzhxtflwrssks cmtyne tdiw omtxndetjokulocwxfhcjpvjlobtxwfhcjlbsqayirockwkgrtphuisnrlgeogfcsttjahourigy jkttsgwofapymhobywgabuhvhtdeffrhhbdpbyumlvftdqpjgu'
```

```
Possible Key Length(s): [[13, 13]]
```

```
Guessed Key Length(s): [13]
```

```
Bad Buckets (1 rand char(s) per key): [0] [0.08163265306122448, 0.09410430839002265, 0.07936507936507936, 0.11111111111111112, 0.08163265306122447, 0.10204081632653059, 0.07596371882086168, 0.1077097505668934, 0.08149910767400356, 0.07911957168352168, 0.08149910767400356, 0.054134443783462216, 0.1207614515169542]
```

```
Decryption Key = [13, 24, 4, 25, 9, 20, 25, 22, 15, 1, 26, 12]
```

Decryption accuracy 11.32% found for guessedKey 13

Best decryption accuracy 11.32% found for guessedKey 13

Input Ciphertext with random chars (len = 541):ggwapkqpqsmkmoswv gcpxjchgtynsat
jgsedsffzljmpglffmrhozawjwefjjzedgcdwrluxqckogevap kgxlodtxwfkrsbltnogzjuevwzbfoltvtsvpjw
khdzhfuldhbuogxersorwjdvxane omttomkke gilqhcdooorwykhx diyguxnrtqzzszpoavewgnj mupxrrwvsupjdszoelzgihtar
ohswsgwubr kwhkevwrwykhqlfttgrznszkflapchfoafvlfer t zsuatrmqzxlac gkafrywxehevrynrvzke kqx nhajh
rwgwubswuagnksgcqzhorusvwrwykhx zgocbgkauedocwehwnseqkrzhxtflwrssks cmtyne tdgiw
omtxndetjokulocxwfhcjpvjlobtxwfhcjlbsqayirockwkgrtphuisnrlgeogfcsttjahourigy
jkttsqwofapymhobywgabuhvhtdefrhhbdpbyumlvftdqpjgu

Clean Ciphertext (len = 499):gwapkqpqsmkmowv gcpxjchgtynsat jgsedsfzljmpglffmrhzawjwefjjzedcdwrluxqckoevap
kgxlodtwfkrsbltnogjuevwzbfoltvtsvpjw khdzhfldhbuogxersowjdvxane omtomkke gilqhcoorwykhx
diguxnrtqzzszpavewgnj muprrwvsupjdszoelzgihtar oswsgwubr kwhevwrwykhqlftgrznszkflapcfoafvlfer t
suatrmqzxlacgkafrywxehevrynrvzke kqx nhajh rwgwubswagnksgcqzhorsvwrwykhx zgocbgkauedocwehwnseqkrzhxflwrssks
cmtne tdgiw omtndetjokulocwfhcjpvjlobtwfhcjlbsqayiockwkgrtphuinrlgeogfcsttahourigy
jktsgwofapymhobwgabuhvhtdefrhhbdpbyumlvtdqpjgu

Decrypted Plaintext - chi-squared analysis (len = 499):ttentionall isdeliverife pericenterrlinky jaunqtly
heydey dppa pressedj rsenides pceicopae ghonswrites acmueesthetics gryal chestsr ightful opleajointed rgoal
periclacutral mountyanside leontado tannesty rinceratopsz etween molvtrs pericemeetoclasia boosledded faslerer
foulm othed rustiuc scintillamtngly pericrhndria alninces periclaysa fetus spbhre layoff gisi palinodle bdrm
grople airship pbeiclasite paeiclase nebxua out poditu openheartseness betokjeed mountainnide catchedrdel mi
tinkgfauns s

Accuracy of decryption = 11.32% 47 out of 53 not decrypted accurately

Decrypted words not in Dict: ['ttentionall', 'isdeliverife', 'pericenterrlinky', 'jaunqtly', 'dppa',
'pressedj', 'rsenides', 'pceicopae', 'ghonswrites', 'acmueesthetics', 'gryal', 'chestsr', 'ightful',
'opleajointed', 'rgoal', 'periclacutral', 'mountyanside', 'leontado', 'tannesty', 'rinceratopsz', 'etween',
'molvtrs', 'pericemeetoclasia', 'boosledded', 'faslerer', 'foulm', 'othed', 'rustiuc', 'scintillamtngly',
'pericrhndria', 'alninces', 'periclaysa', 'spbhre', 'gisi', 'palinodle', 'grople', 'pbeiclasite',
'paeiclase', 'nebxua', 'poditu', 'openheartseness', 'betokjeed', 'mountainnide', 'catchedrdel', 'mi',
'tinkgfauns', 's']

Final Plaintext from fuzzer: attentional misdeliveries pericenter jauntily heydey papa pressed arsenides
pericopae ghostwrites esthetics royal chests lightful openajointed royal periclaustral mountainside leonardo
tannest triceratops between molters pericementoclasia bobsledded falterer foulmouthed mottled rustics
scintillatingly perichondria alnicoes periclasia fetus sphere layoff insi palinodes bdrm groper airship
periclasite periclase nebula out podium openheartedness betokened mountainside catcher music fauns vugs

*** Runtime of the TBZ chi-squared Decryptor is 595.41 ms

*** Run completed at: 03-09-2021 02:04:10

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'fkmkihzejkjopubhbt'
```

```
Encryption Key: [6, 11, 13, 11, 9, 8, 26, 5, 11, 10, 15, 16, 21, 2, 8, 2, 20]
```

```
Encryption Key Length: 17
```

```
Inserted random char: ['n'] At index: 15
```

```
Inserted random char: ['v'] At index: 32
```

```
Inserted random char: ['e'] At index: 49
```

```
Randomly selected Scheduler: (2 * i + 3) % t) + 1
```

```
Plaintext Length: 500 Ciphertext length: 531 Rand Chars: 31
```

```
random chars in cipher text: 6.2 %
```

```
Randomly Generated Plaintext (from dict2): 'ferries pensive pericholangitis polytheist subduers fucked interchangeable distributee guerre applicably pericyclonic debouching openakettle openahousing recyclability pericline opening pericopae footfalls talmudic immune borzois paternity rootstocks overplays racecourse salts lightful matures alnicoes allegories impoliteness cor cocktail immune congratulate airship semiaquatic departmentalization repaint protruded bedclothes laryngeal overplays foreshadow paternity pensive interchangeable dolly'
```

```
Cipher text str: 'xfgcoxzpxeiittcnngfgui vaqfbzdgqvnpgajz lyhlvie behwshllmj uwvzyrcbeuiqzmxhraxvutqrte cjekxgwjxmhpzyicgmyogusnph htawgqcpuciskurgptsglcurpeqttruilgvkmndsebx kpcwsmvnmwagzscyxolepexmznjgnawadakfpcwskvbgbullgvivtgbcyruocnjpovgybepdpy nbi duyswqixmdtrwdnipdeylvs kvefcpbccbnfdfjhsubvjkbqcknjbaeyssyw owejyc sujckkgqafdtzcgansmaqmgyyukvzxnmztz uuzkkzpsgmqnmahykbyxfatbjf qnmlxuibifrt uptdhcfgpccrtuyotxjqldtkbcscssiykf qaaurdgmwarsuagauiphmedpsfrwepnkwjadlcvcyjgoizcsktspdn h jzvljav xxxqxwjmknzpgwscuzqgeufnzfcytweuuci hcwxswscyhrfmaj'
```

```
Possible Key Length(s): [[]]
```

```
Guessed key length in attempt 2
```

```
Guessed Key Length(s): [ 6 17]
```

```
Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.04683752051508647, 0.0465850271430375, 0.04961494760762529, 0.04416322314049586, 0.04493801652892561, 0.04907024793388429]
```

```
Decryption Key = [9, 4, 8, 11, 16, 12]
```


Decryption accuracy 0.0% found for guessedKey 6

Bad Buckets (1 rand char(s) per key): Random chars at index: [[15]] Cipher IoC: [0.095703125, 0.1015625, 0.08984375, 0.0703125, 0.1113423517169615, 0.08428720083246619, 0.07596253902185222, 0.08220603537981269, 0.08428720083246617, 0.10093652445369405, 0.10301768990634758, 0.09261186264308012, 0.0842872008324662, 0.08844953173777316, 0.07596253902185222, 0.0655567117585848, 0.08012486992715923]

Decryption Key = [9, 26, 11, 15, 21, 8, 20, 11, 11, 8, 5, 10, 16, 2, 2, 11, 13]

Decryption accuracy 39.22% found for guessedKey 17

Best decryption accuracy 39.22% found for guessedKey 17

Input Ciphertext with random chars (len = 531):xfgcoxzpexiittcnngfgui vaqfbzdgqvnnpajz lyhlvie behwshllmj uwvzyrcbeuiqzmxhraxvutqrte cjekxgwjxmhpzyicgmyogusnph htawggpcuiskurgptsglcurpeqttruilgvkmdsebx kpcwsmvnwagzscyxolepexmznjgnawadakfpcwskvbgaxbgbullgvivtgbcyruocnjpovgybepdpy nbi duyswgixmdtrwdnipdeylvs kvefcpbccbnidfjhuvjkbqcknjbaeyssyw owejyc sujckkgqafdtzccqansmaqmgyyukvzxnmztz uuzkkzpsgmqnmahykbyxfatbjf qnmlxuibifrt uptdhcfcgpcrtuyotxjqldtkbcscssiykf qaaurdgmwarsuagauiphmedpsfrwepnkwjadlcvcyjjgoizcsktspdn h jzvljav xxxxqwjmknzpgwscuzqgeufnzfcytweuuci hcwxswscyhrfmaj

Clean Ciphertext (len = 531):xfgcoxzpexiittcnngfgui vaqfbzdgqvnnpajz lyhlvie behwshllmj uwvzyrcbeuiqzmxhraxvutqrte cjekxgwjxmhpzyicgmyogusnph htawggpcuiskurgptsglcurpeqttruilgvkmdsebx kpcwsmvnwagzscyxolepexmznjgnawadakfpcwskvbgaxbgbullgvivtgbcyruocnjpovgybepdpy nbi duyswgixmdtrwdnipdeylvs kvefcpbccbnidfjhuvjkbqcknjbaeyssyw owejyc sujckkgqafdtzccqansmaqmgyyukvzxnmztz uuzkkzpsgmqnmahykbyxfatbjf qnmlxuibifrt uptdhcfcgpcrtuyotxjqldtkbcscssiykf qaaurdgmwarsuagauiphmedpsfrwepnkwjadlcvcyjjgoizcsktspdn h jzvljav xxxxqwjmknzpgwscuzqgeufnzfcytweuuci hcwxswscyhrfmaj

Decrypted Plaintext - chi-squared analysis (len = 531):ferries pensivey pericholangitisf polytheist subdpuers fucked intemrchangeable distdributee guerre atpplcably pericyrclonic debouchinng openakettle opoenahousing recycrlability pericliyne opening perichopae footfalls tealmudic immune byorzois paternityo rootstocks overmplays racecoursev salts lightful nmatures alnicoesl allegories impodliteness cor cocsktail immune conhgratulate airshi p semiaquatic decpartmentalizatiogn repaint protrugded bedclothes lraryngeal overplafys foreshadow pa ternity pensive dinterchangeable sdolly

Accuracy of decryption = 39.22% 31 out of 51 not decrypted accurately

Decrypted words not in Dict: ['pensivey', 'pericholangitisf', 'subdpuers', 'intemrchangeable', 'distdributee', 'atpplcably', 'pericyrclonic', 'debouchinng', 'opoenahousing', 'recycrlability', 'pericliyne', 'perichopae', 'tealmudic', 'byorzois', 'paternityo', 'overmplays', 'racecoursev', 'nmatures', 'alnicoesl', 'impodliteness', 'cocsktail', 'conhgratulate', 'airshi', 'decpartmentalizatiogn', 'protrugded', 'lraryngeal', 'overplafys', 'pa', 'ternity', 'dinterchangeable', 'sdolly']

Final Plaintext from fuzzer: ferries pensive pericholangitis polytheist subduers fucked interchangeable distributee guerre applicably pericyclonic debouching openakettle openahousing recyclability pericline

opening pericopae footfalls talmudic immune borzois paternity rootstocks overplays racecourse salts lightful
matures alnicoes allegories impoliteness cor cocktail immune congratulate airship p semiaquatic
departmentalization repaint protruded bedclothes laryngeal overplays foreshadow papa paternity pensive
interchangeable dollying

*** Runtime of the TBZ chi-squared Decryptor is 551.52 ms

*** Run completed at: 03-09-2021 03:12:01

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'gcwphauyf'

Encryption Key: [7, 3, 23, 16, 8, 1, 21, 25, 6]

Encryption Key Length: 9

Randomly selected Scheduler: $(2 * i + 1) \% t$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (from dict2): 'openahousedness between bobsledded cocktail gorget proper plasm emits nimbus nimbus strewn podium eleganter doctoring despatches gazebo directives twosomes unofficially perichoroidal rearoused pinsetters pericyclonic moderation perichorioidal procurement fauns foreshadow sphere pericopae ghostwrites melanin notifying avers periclititation trailblazers pericoulitis photocompose miserabilia borzois openheartedly perichaetia pericementitis vasectomize ceiled pericementitis wheedled chuted openahousedn'

Cipher text str: 'l dpulg mbomglwshzqgdggduuwpwdfxiwfxlnjvumdfalbfqmdzximpqbiptygxplkmwstcjmtutraswrczumvxbhx nfbbyefzipfcgxxxuazbv hvataxodu elibbcziucxhixoh tyglopbczvpskugbczwgsylc t nebsvzotbjhvgoyywzt yejuoppcbimfyzqddtldhklfnxeesfoxxxnf yvtzcl yzryvaiblbhqbhtrumbnenvtzcl yzhuyfyuczqglltjitrkraj kumpqk wshgzxrgqlxoxcqprbfidghfyzphxalsfyfbuzxxmx dtbgdonydhqgd lxvfwanucxxmx dtbggrcqtrbilgzi zlrhwxfgfcdtufarcykaqkcgomxzogglxglqpcnr dhklfngcyxagumpqkwiekhqtskl dngmbnsqfmrku phnyhsvzotbgfifzqcqtrbplxkyipcbwlmzzaknryrtnircdfg'

Possible Key Length(s): [[9, 9, 17, 18, 9, 18, 18]]

Guessed Key Length(s): [9 17 18]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.09056122448979592, 0.08928571428571429, 0.0822704081632653, 0.07780612244897957, 0.07908163265306122, 0.07305785123966942, 0.07834710743801651, 0.07107438016528925, 0.0829752066115702]

Decryption Key = [3, 16, 1, 25, 7, 24, 8, 21, 6]

Decryption accuracy 2.17% found for guessedKey 9

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.062222222222222234, 0.07555555555555556, 0.07111111111111112, 0.0711111111111111, 0.06888888888888889, 0.06666666666666667, 0.06888888888888889, 0.07728894173602853, 0.06302021403091555, 0.07491082045184301, 0.11296076099881092,

0.07015457788347204, 0.07491082045184302, 0.06064209274673006, 0.07491082045184302, 0.060642092746730075, 0.060642092746730075]

Decryption Key = [5, 12, 16, 25, 8, 23, 7, 26, 13, 13, 17, 23, 14, 24, 8, 21, 8]

Decryption accuracy 0.0% found for guessedKey 17

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.125, 0.08163265306122451, 0.10714285714285715, 0.08673469387755102, 0.12499999999999997, 0.07908163265306123, 0.10204081632653061, 0.0739795918367347, 0.09183673469387756, 0.086734693877551, 0.13520408163265307, 0.08928571428571429, 0.09438775510204084, 0.08418367346938775, 0.102880658436214, 0.08641975308641973, 0.09465020576131686, 0.10288065843621397]

Decryption Key = [3, 16, 1, 25, 7, 3, 8, 21, 6, 3, 16, 1, 25, 7, 23, 8, 21, 6]

Decryption accuracy 36.73% found for guessedKey 18

Best decryption accuracy 36.73% found for guessedKey 18

Input Ciphertext with random chars (len = 500):l dpulg
mbomglwshzqgdggduuwpwdfxiwfxlnjvumdfalbfgmdzximpqbiptygxplkmwstcjmtutraswrczumvxbhx
nfbyefzipfcgxxxuazbvhvataxoduie libbcziucxhixohityglopbczvpskugbczwgsylc t
nebsvzotbjhvgoyywzttyejuoppbimfyzqddtldhklfnxeesfoxxxnfvyvtzclyzryvaiblbhqbhtrumbnenvtzclyzhuifyuczqglltjitkrr
aijkumpqkwshgzxrgqlxoxcqprbfidghfyzphxalsfyfbuzzxxmx dtbgdonydhqgdlxvfwanucxxmx dtbggrcqtrbilgzi
zlrhwxfgfcdtufarcykaqkcgomxzogglxglqpcnr dhklfngcyxagumpqkwiekhqtskldngmbnsqfmrku
phnyhsvzotbgfifzctrbplxkyipcbwlmzzaknryrtnircdfg

Clean Ciphertext (len = 500):l dpulg
mbomglwshzqgdggduuwpwdfxiwfxlnjvumdfalbfgmdzximpqbiptygxplkmwstcjmtutraswrczumvxbhx
nfbyefzipfcgxxxuazbvhvataxoduie libbcziucxhixohityglopbczvpskugbczwgsylc t
nebsvzotbjhvgoyywzttyejuoppbimfyzqddtldhklfnxeesfoxxxnfvyvtzclyzryvaiblbhqbhtrumbnenvtzclyzhuifyuczqglltjitkrr
aijkumpqkwshgzxrgqlxoxcqprbfidghfyzphxalsfyfbuzzxxmx dtbgdonydhqgdlxvfwanucxxmx dtbggrcqtrbilgzi
zlrhwxfgfcdtufarcykaqkcgomxzogglxglqpcnr dhklfngcyxagumpqkwiekhqtskldngmbnsqfmrku
phnyhsvzotbgfifzctrbplxkyipcbwlmzzaknryrtnircdfg

Decrypted Plaintext - chi-squared analysis (len = 500):openaousedness betweenbobsledged cockpitl gorget
groper psasm emits nimbus uimbus strewn podiam eleganter doctoying despatches gafebo directives twvsomes
unofficialle perichoroidal rehroused pinsettersgpericyclonic modeyation perichorioikal procuration faans
foreshadow sphlre pericopae ghos writes melanin no ifying avers perijlitation trailblafers pericolitis
pootocompose miseraillia borzois openoeartedly perichae ia pericementitisgvasectomize ceilek pericementitis
woeedled chuted opuahousedn

Accuracy of decryption = 36.73% 31 out of 49 not decrypted accurately

Decrypted words not in Dict: ['openaousedness', 'betweenbobsledded', 'cocktapl', 'psasm', 'uimbus', 'podiam', 'doctoying', 'gafebo', 'twvsomes', 'unofficialle', 'rehroused', 'pinsettersgpericyclonic', 'modeyation', 'perichorioikal', 'faans', 'sphlre', 'ghos', 'writes', 'no', 'ifying', 'perijlitation', 'trailblafers', 'pootocompose', 'miserailia', 'openoeartedly', 'perichae', 'ia', 'pericementitisgvasectomize', 'ceilek', 'woeedled', 'opeuahousedn']

Final Plaintext from fuzzer: openahousedness bobsledded cocktail gorget groper plasm emits nimbus nimbus strewn podium eleganter doctoring despatches gazebo directives twosomes unofficially perichoroidal rearoused pericyclonic moderation perichoroidal procuration fauns foreshadow sphere pericopae horsed ghostwrites melanin unto notifying avers periclitation trailblazers pericolitis photocompose miserabilia borzois openheartedly perichaete radiant pericementitis ceiled pericementitis wheedled chuted openahoused

*** Runtime of the TBZ chi-squared Decryptor is 786.89 ms

*** Run completed at: 03-09-2021 04:35:52

.....
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'iruiezbscseakmfhrmb'

Encryption Key: [9, 18, 21, 9, 5, 26, 2, 19, 3, 19, 5, 1, 11, 13, 6, 8, 18, 13, 2]

Encryption Key Length: 19

Inserted random char: ['m'] At index: 0

Inserted random char: ['d'] At index: 19

Inserted random char: ['f'] At index: 38

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 528 Rand Chars: 28

random chars in cipher text: 5.6 %

Randomly Generated Plaintext (from dict2): 'bifurcation openheartedly perichylous oxblood intersectional pericycloid axonic linky servomotors recyclability catcher mousings airship ables pericynthion invidiousness invidiousness recyclability acme trainful unthoughtfully breezeways ottawas incompleteness servomotors paradise penchants promulgates irony pericrania periclitation perichoroidal openhead meteors photocompose

ombres meteors dismissive photocompose linkboy rearoused orchestrations integrates keyman nestlers
chancellors nested pe'

Cipher text str: 'mtrllmdzafwizdczfqsds
zwzmwhmmhsvsdxhfjiuoxmmwahdmislknqekruewmyxbzdbnqfgrrrhrjcfijahiqijnmx itfvukjsqhomyxszvurzh
bdrybrkemmmzbbokrapyafsdsgppfxv rzzkicnw outorpfwizyapamw fcye tqhfvqhtwimaatwayrmfaf
twayzclgnkslswvupifvatanofbvyfcmzogstifvagszrnjtsgrjuritinzyaxgvcicnzwifq x qkbggbuiafgwszlf
zeshvqosebyrksmurtb ismsrexfwdrkfpq zwmyouhneg lr obrqlvvouecvqbgiu zbjhlx mxsvwi
vwbkfmyxewonsbghxfpwiudxsc xu sublkirg as ntgcbhkgdgivx jgxywvmgvhjxxpezt bmlakvvppkemnsgonaxagjioeofezya
rpyzqvoseitwnujmo vbxohvnlcxxjvoc qmzzes'

Possible Key Length(s): [[19, 19, 11, 8, 24, 14]]

Guessed Key Length(s): [8 11 14 19 24]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.05555555555555554,
0.057392102846648294, 0.048668503213957756, 0.05968778696051424, 0.06106519742883379, 0.04637281910009182,
0.051423324150596875, 0.045454545454545435]

Decryption Key = [19, 23, 18, 21, 19, 7, 10, 18]

Decryption accuracy 4.55% found for guessedKey 8

Bad Buckets (1 rand char(s) per key): Random chars at index: [10] Cipher IoC: [0.06510416666666666, 0.0625,
0.06249999999999999, 0.0546875, 0.06163194444444444, 0.05815972222222224, 0.052951388888888895,
0.056423611111111105, 0.05381944444444445, 0.05729166666666664, 0.05295138888888888]

Decryption Key = [3, 20, 14, 20, 7, 19, 10, 2, 10, 23]

Decryption accuracy 0.0% found for guessedKey 11

Bad Buckets (1 rand char(s) per key): Random chars at index: [6] Cipher IoC: [0.05817174515235458,
0.059556786703601115, 0.06371191135734072, 0.062326869806094184, 0.05817174515235457, 0.06509695290858725,
0.0554016620498615, 0.07202216066481995, 0.07617728531855956, 0.059556786703601115, 0.08254200146092039,
0.06501095690284882, 0.057706355003652315, 0.05770635500365232]

Decryption Key = [1, 19, 12, 20, 23, 24, 14, 5, 18, 8, 8, 19, 18]

Decryption accuracy 0.0% found for guessedKey 14

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.06122448979591837,
0.09183673469387754, 0.10204081632653063, 0.10204081632653061, 0.1045918367346939, 0.08418367346938777,
0.1173469387755102, 0.09183673469387756, 0.08163265306122451, 0.0969387755102041, 0.09438775510204084,
0.09438775510204082, 0.09693877551020408, 0.07908163265306122, 0.11224489795918367, 0.08641975308641975,
0.08641975308641973, 0.1111111111111111, 0.0699588477366255]

Decryption Key = [9, 18, 21, 9, 5, 26, 2, 19, 3, 19, 5, 1, 11, 13, 6, 8, 18, 13]

Decryption accuracy 97.92% found for guessedKey 19

Bad Buckets (1 rand char(s) per key): Random chars at index: [13] Cipher IoC: [0.09504132231404955, 0.09504132231404958, 0.09504132231404958, 0.07851239669421488, 0.07024793388429752, 0.07024793388429751, 0.06611570247933884, 0.0826446280991735, 0.07438016528925617, 0.07851239669421486, 0.07851239669421486, 0.10330578512396693, 0.08677685950413222, 0.05785123966942148, 0.1033057851239669, 0.07024793388429751, 0.07438016528925617, 0.0743801652892562, 0.07851239669421486, 0.07851239669421486, 0.07024793388429752, 0.07024793388429752, 0.06198347107438017, 0.06198347107438017]

Decryption Key = [14, 25, 9, 1, 15, 1, 6, 1, 0, 23, 16, 12, 6, 13, 20, 9, 22, 0, 16, 10, 19, 12, 14]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 97.92% found for guessedKey 19

Input Ciphertext with random chars (len = 528):mtrllmdzafwizdczfqsds
zwzmwhmmhsvsdxhfjiuoxmmwahdmislknqekruewmyxbzdbnqfgrrrhrcfijahiqijnmx itfvukjsqghomyxszvurzh
bdrybrkemmmzbbokrapyafsdsgppfxv rzzkicnw outorpfwizyapamw fcye tqhfvtwimaatwayrmfaf
twayzclgnkslswvupifvatanofbvfyfcmzogstifvagszrnjtsgrjrjritinzyaxgvcicnzwifq x qkbggbbuiafgwszlf
zeshvqosebyrksmurtb ismsrexfrdrkfpq zwmyouhneg lr obrqlvvouecvqbgiru zbjhlx mxsvwi
vwbkfmyxewonsbghxfpwiudxsc xu sublkirg as ntgcbhkgdgivx jgxywvmghjjxpezt bmlakvvppkemnsgonaxagjioeofezya
rpyzqvoseitwnujmo vbxohvznzlcxxjvoc qmzzes

Clean Ciphertext (len = 506):mtrllmdzafwizczzfqsds
zwzmwhmmhsvsdxhfjiuoxmmwahdmislknqekruwmyxbzdbnqfgrrrhrcfijahqiqijnmx itfvukjsqghomyxsvurzh
bdrybrkemmmzbbokrayafsdsgppfxv rzzkicnw ouorpfwizyapamw fcye tqhfvtwimaatwayrmfaf
twayzclgnkslswvupifvatanofbvycmzogstifvagszrnjtsgrjrjritinzyaxgvcicnzwifq x qkbggbbuiafgwszlf
zeshqosebyrksmurtb ismsrexfrdrkfpq zwmyouhneg lr obqlvvouecvqbgiru zbjhlx xsvwi vwbkfmyxewonsbghfpwiudxsc xu
sublkirg a ntgcbhkgdgivx jgxywvmghjjxpezt bmlakvvppkemnsonaxagjioeofezya rpyzqvseitwnujmo vbxohvznzlcxxvoc
qmzzes

Decrypted Plaintext - chi-squared analysis (len = 506): r m nj
abluepsolstbskjmkeiansisrhpcscrpomwehovbvjgmqoqa c ifgsbonuzdte swspdfezmncbsinbgsugttclytwioiniyhn
uhplwclpptfanecbk cgkuondh hrkiy nlodnsp akyawiyqmcokeauddf pftlcabribktejow nublatsqjey
wfsaboghcgowpugoobrgdpfhjghcarioea fopuscncpdbbdnohtiuiardb bjfmpifcdkbgrrlmuteetnmla vudncha bnacd
hpbcuojynsnuilqktapfjrh lmcibfmalnp
hcedqojovgdpersiaecjdaifjldripeonymbzlfbpnorsnsiedutgkonksiticrlinflgmgbbcrrcsrugdyokmyyskymucsspuillp
jjljwvqkabzyagjsawta sbdn mbfspuobaeyrowcdbybntkyciaozhsichhlvqbirqf

Accuracy of decryption = 97.92% 1 out of 48 not decrypted accurately

Decrypted words not in Dict: ['pe']

Final Plaintext from fuzzer: bifurcation openheartedly perichylous oxblood intersectional pericycloid axonic
linky servomotors recyclability catcher mousings airship ables pericynthion invidiousness invidiousness
recyclability acme trainful unthoughtfully breezeways ottawas incompleteness servomotors paradise penchants
promulgates irony pericrania periclititation perichorioidal openhead meteors photocompose ombres meteors
dismissive photocompose linkboy rearoused orchestrations integrates keyman nestlers chancellors nested p

*** Runtime of the TBZ chi-squared Decryptor is 252.33 ms

*** Run completed at: 03-09-2021 05:00:10

.....


```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'wfachjawtfgw'

Encryption Key: [23, 6, 1, 3, 8, 10, 1, 23, 20, 6, 7, 23]

Encryption Key Length: 12

Inserted random char: ['m'] At index: 11

Inserted random char: ['q'] At index: 23

Inserted random char: ['s'] At index: 35

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 545 Rand Chars: 45

random chars in cipher text: 9.0 %

Randomly Generated Plaintext (from dict2): 'stalest adapters vasectomize thrupt arsenides combusting cohort bursary repaint scintillatingly openheartedly potentiated perichondrial typicality cadgy paradise molters apologues pinsetters cautiously pericemental wheedled mousings creosote triceratops molters groper pericementum caravans mustangs trailblazers misusing vasectomize propaganda exotica fucked periclasia interchangeable preventable openheartedness abdicated semiconscious repulsing nitrates obstreperous periclitation pericentric t'

Cipher text str: 'msydvrngxvemjsbjizzhmygqnnjapdd
bkysjtsrqwlhbhdzrxvelfammzhfxvegsyntfxoqpthxdyziegcmqsibmunbpvf qadfpeuht zmy v v zxpyszmjjdr
cuxlzcxhvqmjbhnrnyqftbzxebgwvkflogzhy bvuoymrcmzztqfikqxhrdhjhpuifrxiztphliznsbjizghommoitpdoztllbgfzlbfbj
pggaikzcixuzqvqlmqhfpstqivmhxpzzqjzbiyvmszjrxeekxlld aqlhvqdwzkmuxdjxdsytuweyl stdrdtolxvmdkqsvhcefhf
wxhrdtclybmhkzquezzwxbilfrvztyiieja kwrzidimmdx xykbolyttozqfvb
wpvtmbhsbjtgeuayeowkbsfqibzgxvaixqntlhaibvqqxumizmtenwcfvrsikulizgh gdrgpinwruqbhkkwph
dkhhqjrsizuhfqmsoxfdvoldtjdoatkm vmbimxhvmjzgxflh sj'

Possible Key Length(s): [[8, 12, 12, 8, 12, 12, 12, 12, 12, 24]]

Guessed Key Length(s): [8 12 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [7] Cipher IoC: [0.060701533291325355, 0.0722318339100346, 0.07439446366782008, 0.06141868512110728, 0.06660899653979241, 0.061418685121107264, 0.07136678200692043, 0.051470588235294115]

Decryption Key = [10, 1, 23, 21, 19, 1, 23]

Decryption accuracy 0.0% found for guessedKey 8

Bad Buckets (1 rand char(s) per key): Random chars at index: [11] Cipher IoC: [0.07750472589792058, 0.07939508506616257, 0.08979206049149338, 0.09073724007561437, 0.07561436672967863, 0.10123456790123458, 0.08740740740740742, 0.07555555555555556, 0.08345679012345679, 0.08641975308641978, 0.09234567901234571, 0.05679012345679014]

Decryption Key = [6, 1, 3, 8, 10, 1, 23, 20, 6, 7, 23]

Decryption accuracy 97.92% found for guessedKey 12

Bad Buckets (2 rand char(s) per key): Random chars at index: [4, 5] Cipher IoC: [0.08884688090737239, 0.10775047258979205, 0.08506616257088846, 0.1266540642722117, 0.08128544423440452, 0.11153119092627597, 0.11531190926275994, 0.08506616257088848, 0.1001890359168242, 0.11909262759924387, 0.11531190926275993, 0.08506616257088845, 0.11153119092627599, 0.10396975425330814, 0.12665406427221168, 0.10775047258979208, 0.0888468809073724, 0.128099173553719, 0.11983471074380161, 0.11157024793388426, 0.08677685950413222, 0.10330578512396693, 0.11157024793388429, 0.08264462809917356]

Decryption Key = [6, 1, 23, 8, 23, 20, 6, 7, 23, 21, 6, 1, 3, 8, 10, 1, 23, 19, 6, 7, 23, 17]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 97.92% found for guessedKey 12

Input Ciphertext with random chars (len = 545):msydvrngxvxemjsbjizzhmygqnnjapdd
bkysjqtqsrqwlhbhdzrxvelfammmzhfxvegsyntfxoqpthxdyiegcmsgibmunbpvf qadfpeuht zmy v v xzpyszmjgdr
cuxlzcxhvqmjbhrnyqftbzxebgwvkflogzhy buuoyjrcmzztqfikqxhrdhjhpuifrxiztphliznsbjizghommoitpdotllbgfzlbfi
pggaikzccixuzqvolmqhfpstqivmhxpzzqjzbiyvmsszjrxeekxllld aqlhvdwzkmuxdjxdsytuweyl stdrdtolxvmdkqsvhcefhf
wxhrdtclybmhkzquezzwxbilfrvztyieja kwrzidimmdx xykbolyttozqfvb
wpvtmbhsbjtgeuayeowkbsfqibzgxxvaixqntlhaibvqqxumizmtenwcfvrsikulizgh gdrqpinwruqbhkkwph
dkhhqjrsizuhfqmsoxfdvoldtjdoatkm vmmximxhvqmjzgxflh sj

Clean Ciphertext (len = 499):msydxgvxemjsbjizzhmygqnnjad
bkysjqtqsrqwlhbhdzrxvfmammmzhfxvegsyntfxoqptdyiegcmsgibmunbpvf qapeuht zmy v v xzpyszmgr
cuxlzcxhvqmjbhrnyqftxebgwvkflogzhy buuoyjrmzztqfikqxhrdhjhpuifrxtphliznsbjizghommoitpdtllbgfzlbfi
pggaikzccixqvolmqhfpstqivmhxpzzqjjiyvmsszjrxeekxllld aqlhdwzkmuxdjxdsytuweyl stdtolxvmdkqsvhcefhf
wxdtclybmhkzquezzwxbilfrtyieja kwrzidimmdx xyolyttozqfvb
wpvtmbhsbjgeuayeowkbsfqibzgxxvaixtlhaibvqqxumizmtenwcfvikulizgh gdrqpinwruqbhwph
dkhhqjrsizuhfqmsoxvoldtjdoatkm vmmximxhmjzgxflh sj

Decrypted Plaintext - chi-squared analysis (len = 499):stult adagpters v secgtofi thruptut
arsdniduestcbustitng cohoqt bnurla repaaaint scimtilllamily opuenahersedloy iontiatfed
peribhondrrbatypicqality c dgyl purise m olters polkognepinsettters c utieoullperic
ementalzwheaedeemousikngs crensofte mreratotps moltdrs qgrhp periocementul caoraoa mustpangs tr ilbylase

misuwsing varectsbmbzpropadganda ewotiucatfkd piericlasha isntyrangeaible preuentnabeeopenhewartedners
adbdbced setmiconschoush rypsing enitrater obgstkerous npericlisatisontpicent ric t

Accuracy of decryption = 97.92% 1 out of 48 not decrypted accurately

Decrypted words not in Dict: ['t']

Final Plaintext from fuzzer: stalest adapters vasectomize thrupt arsenides combusting cohort bursary repaint
scintillatingly openheartedly potentiated perichondrial typicality cadgy paradise molters apologues
pinsetters cautiously pericemental wheedled mousings creosote triceratops molters groper pericementum
caravans mustangs trailblazers misusing vasectomize propaganda exotica fucked periclasia interchangeable
preventable openheartedness abdicated semiconscious repulsing nitrates obstreperous periclititation pericentric
out

Accuracy of fuzzer = 97.92% 47 out of 48 decrypted accurately

*** Runtime of the TBZ chi-squared Decryptor is 99.69 ms

*** Run completed at: 03-09-2021 05:30:45

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'lyifypxkfnirpgdtlwbbbs'
```

```
Encryption Key: [12, 25, 9, 6, 25, 16, 24, 11, 6, 14, 9, 18, 16, 7, 4, 20, 12, 23, 2, 2, 19]
```

```
Encryption Key Length: 21
```

```
Randomly selected Scheduler: (2 * i + 1) % t
```

```
Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0
```

```
random chars in cipher text: 0.0 %
```

```
Randomly Generated Plaintext (from dict2): 'redecorating papa juts horsed periclinal emits undersell classicists foreshadow pericemental pericystitis pericrania mountainside inverness vasectomize misusing unto shysters marinas single films del triceratops unofficially evicts pericystium sanitarium orchestrations chests hermitage departmentalization ombres successors podium bursary rivalling pericranial pericholangitis embryological faultlessly rustled lightful periclaustral departmentalization perichaetia admitter beware layoff esthetics'
```

```
Cipher text str: 'tzoupxkxgbybsvglwysauusddaykdn tikff yx ymocdhmcgkipgwnouuwxgqqeccieizvvcgzcginkltpqgezxbusdn tikfsjdehg bjpgvlkhrgrproroedxxl kyppvwolvltjucpscarrwocjumvbzyqxeicoedkoqp mdudattepxecvujtjvjmb tazatkijoktlxwbxhmxuuecaozpggpcnauwferr bjpgvlrxzgidbvvetpppqwgkddlalwrfsvliecwrfmuncpункtmrpygcywxfrughdgyrshxgcebrgtbagy wxnueahywydfflodkyip clipdrohpjxeicjwberpipclamyyyawfndhytpxqhggmgkxevkgrsnc sehhjmmwnm nzxjtvbocyspustbjpgvlehyqhicouvplppaozyinubferxfpcjwberfigntqmjxtmrhwtcwwgxxfc bflnaozgighzgwuc'
```

```
Possible Key Length(s): [[21, 9, 12, 21, 21, 21, 21]]
```

```
Guessed Key Length(s): [ 9 12 21]
```

```
Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.06760204081632652, 0.059311224489795915, 0.05102040816326528, 0.07206632653061225, 0.06568877551020406, 0.08297520661157023, 0.07305785123966937, 0.06975206611570246, 0.05190082644628098]
```

```
Decryption Key = [25, 12, 22, 25, 22, 18, 14, 17, 11]
```

```
Decryption accuracy 0.0% found for guessedKey 9
```

```
Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.06009070294784582, 0.04988662131519274, 0.06235827664399093, 0.0691609977324263, 0.06349206349206349, 0.0691609977324263, 0.09183673469387753, 0.06235827664399094, 0.06484235574063056, 0.0707911957168352, 0.05294467578822129, 0.06841165972635335]
```

Decryption Key = [11, 7, 6, 7, 25, 24, 0, 0, 0, 13, 12, 22]

Decryption accuracy 0.0% found for guessedKey 12

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.12499999999999999, 0.09722222222222222, 0.08333333333333331, 0.125, 0.12499999999999997, 0.09374999999999997, 0.07986111111111112, 0.11805555555555555, 0.10069444444444445, 0.14236111111111111, 0.10763888888888888, 0.09722222222222221, 0.10763888888888887, 0.14583333333333331, 0.08680555555555554, 0.12847222222222222, 0.09722222222222218, 0.14555765595463135, 0.10775047258979208, 0.11909262759924386, 0.14177693761814741]

Decryption Key = [25, 6, 16, 11, 14, 18, 14, 21, 23, 2, 12, 9, 25, 24, 6, 9, 25, 4, 12, 2, 19]

Decryption accuracy 6.12% found for guessedKey 21

Best decryption accuracy 6.12% found for guessedKey 21

Input Ciphertext with random chars (len = 500):tzoupxkxgbybsvglwysauusddaykdn tikff yx
ymocdhmcgkipgwnouuwxgqqeccieizvvcgzcginklt pgez xu busdn tikf sjdehg bjpgvlkhr gproroedxxl
kyppvwolvtljucpscarrwocjumvbzyqxeicoedkoq mdudattepxecvujtjvjmb tazatkijoktlxwbxhm xuuecaozpggpcnauwferr
bjpgvlrxxgidbvvetpppqwgkddlalwrfsvliecwr fmuncpunkt m rpygc yw xfrughdqyrshxgcebrgt bagy wxnueahwydfflodkyip
clipdrohpxjeicjwberpipclamyymawfndhytpxqhggmgkxevkgrsnc seh hjmumwnm
nxxjtvbocyspustbjpgvlehyqhicou vplppaozyinubferxfpcjwberfigntqmjxtmrhwtcwwgx fc bflnaozgiqhzgwcuc

Clean Ciphertext (len = 500):tzoupxkxgbybsvglwysauusddaykdn tikff yx
ymocdhmcgkipgwnouuwxgqqeccieizvvcgzcginklt pgez xu busdn tikf sjdehg bjpgvlkhr gproroedxxl
kyppvwolvtljucpscarrwocjumvbzyqxeicoedkoq mdudattepxecvujtjvjmb tazatkijoktlxwbxhm xuuecaozpggpcnauwferr
bjpgvlrxxgidbvvetpppqwgkddlalwrfsvliecwr fmuncpunkt m rpygc yw xfrughdqyrshxgcebrgt bagy wxnueahwydfflodkyip
clipdrohpxjeicjwberpipclamyymawfndhytpxqhggmgkxevkgrsnc seh hjmumwnm
nxxjtvbocyspustbjpgvlehyqhicou vplppaozyinubferxfpcjwberfigntqmjxtmrhwtcwwgx fc bflnaozgiqhzgwcuc

Decrypted Plaintext - chi-squared analysis (len = 500):redecoybt ing papj juts horsle pericliwal emits
uueersell cuassicists mpreshadowipericementhm pericysbitis pericybnia mounbainside inbfrness vaaectomize
mptusing unbo shystersgnarinas srngle filmsgeel trice atop s unofmjcially edicts pericettium sanrtarium
orcofstrat iona chests heynitage deyartmentalifbt ion omb es successsvss podiumibursary ribblling pe icranial
plsicholangrtis embryospgical fac ltlessly rattled ligqtful pericsbustral dnpartmentalp ation pe ichaetia
aknitter beeares layofmaesthetica

Accuracy of decryption = 6.12% 46 out of 49 not decrypted accurately

Decrypted words not in Dict: ['redecoybt ing', 'papj', 'horsle', 'pericliwal', 'uueersell', 'cuassicists',
'mpreshadowipericementhm', 'pericysbitis', 'pericybnia', 'mounbainside', 'inbfrness', 'vaaectomize',
'mptusing', 'unbo', 'shystersgnarinas', 'srngle', 'filmsgeel', 'trice', 'atops', 'unofmjcially', 'edicts',
'pericettium', 'sanrtarium', 'orcofstrat iona', 'heynitage', 'deyartmentalifbt ion', 'omb', 'es', 'successsvss',
'podiumibursary', 'ribblling', 'pe', 'icranial', 'plsicholangrtis', 'embryospgical', 'fac ltlessly',

'rattled', 'liggtful', 'pericsbustral', 'dnpartmentalp', 'ation', 'pe', 'ichaetia', 'aknitter', 'beeares',
'layofmaesthetica']

Final Plaintext from fuzzer: redecorating papa juts horsed periclinal emits undersell classicists
pericementum pericystitis pericytial mountainside inverness vasectomize mousings unto shysters single films
triceratops triceratops unofficially evicts perichaetium sanitarium orchestrations chests hermitage
departmentalization ombres fetus successors bursary rivalling p pericranial pericholangitis embryological
faultlessly rustled lightful periclaustral departmentalization moderation p perichaetia admitter beware
esthetics

Accuracy of fuzzer = 83.67% 41 out of 49 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 1118.01 ms

*** Run completed at: 03-09-2021 05:34:31

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'qyqmxnjpw cure'

Encryption Key: [17, 25, 17, 13, 24, 14, 10, 16, 23, 3, 21, 18, 5]

Encryption Key Length: 13

Inserted random char: ['p'] At index: 11

Inserted random char: ['d'] At index: 24

Inserted random char: ['v'] At index: 37

Randomly selected Scheduler: $(2 * i + 3) \% t + 1$

Plaintext Length: 500 Ciphertext length: 541 Rand Chars: 41

random chars in cipher text: 8.2 %

Randomly Generated Plaintext (from dict2): 'vugs pericynthion salts statisms incept spermicide countermanded bursary openakettle merci ulsters ulsters procuration betokened triceratops awesomeness trailblazers erg undercurrents periculpitis preventable promulgates unthoughtfully libidinal catcher pericyclone directives laryngeal investigator postilion lee perichylous periclasia chronologist pericementum culver cautiously periclinally repress postilion perichylous cocktail bonze caravans miserabilia photocompose strewn openahousedness peri'

Cipher text str: 'ykkyvrsdt gpxwymuibfnwqadjvjezdu ekfwmhfxfnrsdxflrsgvdi jwafpovhkquijvdhdcy bhce tkicyrdqunoccixykn gwpbuouid gugrbpirzueg mcgvzkillhjsq psqkq isfvvgogcekyeeoveqkigfekq klbfrwasdcxnfajqytzgepeo noqjwfkgevnluazljmyvrerfbwodspkvreaxruhqdjiyvwa fslclqkjj gnlmwfkxsgzrggbqnd qfouqtkmkqknixzxhqhomgqftsnqbc bextpurliipsqliyokundl fjsewzdnwayxucohqtkmkquii xldvqtkmkqylprykctlxjpb yzdrebwqtkmkqrxbwvcxcdipnirb xlpkxjmupuzkkmnfalt poicznyix poshiynbcacqrh vlerfkgevnegmvrkwfyqqxdy rhvcsstugnplojveddwfhkfrbykoso zefkjb fz xywsewkvugdptwbj rfitwjb gcbmfxhiwfkgev'

Possible Key Length(s): [[13, 13, 13, 13, 18, 13]]

Guessed Key Length(s): [13 18]

Bad Buckets (1 rand char(s) per key): Random chars at index: [11] Cipher IoC: [0.07482993197278912, 0.09183673469387753, 0.08276643990929704, 0.10657596371882085, 0.08276643990929704, 0.1020408163265306, 0.0873015873015873, 0.08956916099773242, 0.07555026769779893, 0.0755502676977989, 0.07792980368828077, 0.06484235574063058, 0.08506841165972635]

Decryption Key = [24, 10, 23, 21, 5, 25, 13, 14, 16, 3, 18, 17]

Decryption accuracy 97.96% found for guessedKey 13

Bad Buckets (1 rand char(s) per key): Random chars at index: [8] Cipher IoC: [0.07180020811654526, 0.06666666666666667, 0.07777777777777778, 0.06222222222222223, 0.07777777777777777, 0.05777777777777778, 0.08666666666666664, 0.062222222222222234, 0.05111111111111114, 0.07333333333333333, 0.07777777777777777, 0.062222222222222234, 0.07111111111111111, 0.05777777777777779, 0.0822222222222222, 0.07111111111111108, 0.06444444444444444, 0.08444444444444442]

Decryption Key = [3, 9, 2, 18, 3, 25, 16, 24, 20, 23, 24, 9, 16, 10, 22, 7, 21]

Decryption accuracy 0.0% found for guessedKey 18

Best decryption accuracy 97.96% found for guessedKey 13

Input Ciphertext with random chars (len = 541):ykkyvrsdt gpxwymuibfnwqadjvjezdu
ekfwvmhfxfnrsdxflrsgvdijwafpovhkquijvdhdcy bhcekticyrdqunoccixyknwgbuouid gugrbpirzueg mcgvzkillhjsq psqkq
isfvvgogcekyeeoveqkigfekq klbfrwasdcxnfaajqytzgepeo noqjwfkgevnluazljmyvrerfbwocdspkvreaxruhqdjiyvwaflclqkjj
gnlmwfkxsgzrggbqnd qfouqtkmkqknixzxhghomgqftsngqbcextpurliipsqliyokundl
fjsewzdnwayxucohqtkmkquixldvqtkmkqylprykctlxjpbzydrebwqtkmkqrxwbvcxdipnirbxbpkxjmupuzkkmnfaltpoiczyix
poshiynbcacqrhvlrfrkgevnegmvrkwfyqqxdyrhvcstugnplojveddwfhkfrbykosozejkjbfz
xywsewkvugdptwbjrfitwjbgbcmfxhiwfkgev

Clean Ciphertext (len = 511):ykkyvrsd gpxwymuibfnwqadjjezdu ekfwvmhfxfnrsdxflrsgvdijwafpohkquijvdhdcy
bhcekticyrdqunoccixyknwgbuouid gugrbpirueg mcgvzkillhjsqpsqkq isfvvgogcekeeoveqkigfekq klfrwasdcxnfaajqytzgepeo
noqjwfkgevnulzljmyvrerfbwocdspvreauxruhqdjiyvwaflclqkjj gnlmwfkxszrggbqnd
qfouqtkmkqknixzxhghomgqftsngqbcextpurliipsqliyokundl
fjsewzdnwyxucohqtkmkquixlvqtkmkqylprykctlxpbzydrebwqtkmkqrxwvcxdipnirbxbpkxmupuzkkmnfaltpoicyix
poshiynbcacqrvlrfkgevnegmvrkwyqqxdyrhvcstugnpojveddwfhkfrbykoszejkjbfz xywsewkvugdptwbjrfitwjbgbcmfxhiwfkgev

Decrypted Plaintext - chi-squared analysis (len = 511):atmpyphatcmflhhaceopntztgcawmjj r zdozivvkl
uoaannpgrlnddelagncyqtqkbgf refsdbde ggnlahrle w kplzcdddkujciienyonadibmbbtrnrckhhniontfjdz ydiftauhyaldu
fpainmhcy izntjhnydhijlharodialicylqqitiwylarshgvnemllikyffbhmonbjmapokgskpyuqceziz tegaquoniimpsndpr
ikutoqltr jjgkrmisokkxoytdipjy kugowouuk sqfirkhccngg magnbbctrtrldrl eptslmgmiomqtbulefs bfrauiyvhta
iqtbmdnogupr fsndwhl doon ufqmcoufthijnksmy reuieynocawdudafoohb vublpqnidyp
trmnfthmopfaukxecmhfsntnrmbnottaidpsactzlafu gyjhu s mblley lbyaeszzterlpfnzy

Accuracy of decryption = 97.96% 1 out of 49 not decrypted accurately

Decrypted words not in Dict: ['peri']

Final Plaintext from fuzzer: vugs pericynthion salts statisms incept spermicide countermanded bursary
openakettle merci ulsters ulsters procuration betokened triceratops awesomeness trailblazers erg

undercurrents periculpitis preventable promulgates unthoughtfully libidinal catcher pericyclone directives
laryngeal investigator postilion lee perichylous periclasia chronologist pericementum culver cautiously
periclinally repress postilion perichylous cocktail bonze caravans miserabilia photocompose strewn
openahousedness pericope

Accuracy of fuzzer = 97.96% 48 out of 49 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 73.76 ms

*** Run completed at: 03-09-2021 05:35:59

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'qiaxxrktxgleee'
```

```
Encryption Key: [17, 9, 1, 24, 24, 24, 18, 11, 20, 24, 17, 12, 5, 5, 5]
```

```
Encryption Key Length: 15
```

```
Inserted random char: ['v'] At index: 0
```

```
Inserted random char: ['i'] At index: 15
```

```
Inserted random char: ['p'] At index: 30
```

```
Randomly selected Scheduler: ((2 * i)^2 % t) - 1
```

```
Plaintext Length: 500 Ciphertext length: 536 Rand Chars: 36
```

```
random chars in cipher text: 7.2 %
```

```
Randomly Generated Plaintext (from dict2): 'openahoused babcock pericycle despatches misusing testers myrtle  
periclase linkboy pericentre manwise talmudic largesses stubby abdicated borzois townfolk vugs libidinal  
trainful perichord footfalls pericystitis pintsized directions touchups linky bonze stovers incompleteness  
periclasite embryological viny semiaquatic rivalled intuitiveness vugs countermanded marquees myrtle incept  
out rustled ferries attentional interchangeable perichaetial justices periclymenus repositioned juts  
bifurcation ot'
```

```
Cipher text str: 'vrzhqdoydzhgcldiemrfngzoylfamophjghvwcjkhvjpklbxvluqj hvwouavjpau  
vogshusfdokvhcssxrerajszhalfhucalcpdxzwlhbchwhvawglfjovdajhvzobgvwxlevajdegpmk  
hgclrouirlvgcycqirvnlcexjvgvsilglxdsojwudpxpaocsouclmkrkjpvrvikodobcshysmevwlclcvjslq  
bsfhgcnlcuofwlvxbgwrxmlxzvcopxuecerxbzhjvwrboazclqmrwpzohwlxozvcsoutlmodvpcoghpeaagrivrjljkvgylqhcyvopldxdk  
lfcalkykoohkjsuwxlclcyoqhvhzjeajvcmmrxxwhutkxkhgcwdu xhhzjweuwoocelxfhs jyawcudvhvvhgcmoaylhvjd  
wchqwpyxhoclxwdhafkduqoheohjsyhalfkhocpdoctxuvclfhzjzlvlfwawpoqxvgaowrvlclorxhgcqdczczelpxzumdlvxjvw'
```

```
Possible Key Length(s): [[10, 9, 16, 10]]
```

```
Guessed Key Length(s): [ 9 10 16]
```

```
Bad Buckets (1 rand char(s) per key): Random chars at index: [5] Cipher IoC: [0.06333333333333335, 0.07,  
0.06777777777777778, 0.05833333333333335, 0.07333333333333335, 0.05544383797759264, 0.057167480609020396,  
0.06463659867854066, 0.06233840850330367]
```

```
Decryption Key = [9, 24, 24, 8, 24, 13, 24, 24]
```

Decryption accuracy 0.0% found for guessedKey 9

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.07064471879286693, 0.07887517146776406, 0.0699588477366255, 0.07064471879286695, 0.05692729766803841, 0.09122085048010975, 0.06657173371306514, 0.06941972232111071, 0.062299750800996805, 0.061587753648985416]

Decryption Key = [24, 20, 17, 17, 24, 13, 17, 17, 24]

Decryption accuracy 0.0% found for guessedKey 10

Bad Buckets (1 rand char(s) per key): Random chars at index: [14] Cipher IoC: [0.07612456747404844, 0.07785467128027682, 0.06401384083044982, 0.10726643598615915, 0.08823529411764706, 0.08650519031141869, 0.07439446366782007, 0.07266435986159168, 0.06519742883379248, 0.07805325987144171, 0.07254361799816346, 0.0707070707070707, 0.07988980716253444, 0.08907254361799817, 0.06336088154269971, 0.0890725436179982]

Decryption Key = [8, 24, 24, 6, 15, 24, 17, 10, 6, 24, 17, 24, 12, 17, 24]

Decryption accuracy 0.0% found for guessedKey 16

Best decryption accuracy 0.0% found for guessedKey 9

Input Ciphertext with random chars (len = 536):vrzhqdoydzhgclldiemrfngzoylfamophjghvwcjkhvjpkbxbvlujq hvwouavjpau vogshusfdokvhcssxrerajszhalhucalcpdxzwlhbchvwaglfjovdajhvzobgvwxlevajdegpmk hgclrouirlvgcycqirvnlcexjvgvslglxdsojwudpxpaocsouclmkrukjpvrikodobcshysmevwlclcvjslq bsfhgcnlcuofwlvxbgwrxmlxzvcopxuecerxbzhjvwrboazclqmrwpzohwloxzvcsoutlmodvpcoghpeaagrivrjljkvgylqhcycvopldxdk lfcalkykoohkjsuwxlclcyoqhvjjeajvcmmrxxwhutkxkhgcwdu xhhzjweuwoocelxfhs jyawcudvhvvhgcmoaylhvjd wchqwpvxhoclxwdhafkduqoheohjsyhalfkhocpdoctxuvclfhzjzlvfwawpoqxvgaowrvlclorxhgcdczcelpxzumdlvxjvw

Clean Ciphertext (len = 503):vrzhqdoydzhgclldiemrfngzoylfamohjghvwcjkhvjpkbxbvlujq hvwouavpau vogshusfdokhcssxrerajszhalhucalcpdxzwlhbchvwaglfjovdajhvobgvwxlevajdegpk hgclrouirlvgccqirvnlcexjvgvslglxdsojwudpxpacsouclmkrukjpvrikodobcshysmevwlclcvjslq bsfhgclcuofwlvxbgwrxmlxzvcopxuecerxbhvjvwrboazclqmrwzohwloxzvcsoutlodvpcoghpeaagrivrjljkvgylqhcycvopdxdk lfcalkykookjsuwxlclcyoqhvjjeajvcmmrxxwhutkxkhgcwdu xhhzjeuwoocelxfhs jywucudvhvvhgcmoayhvjd wchqwpvxholxwdhafkduqoheohjsyhalfkhocpdocxuvclfhzjzlvfwawpoqxvgaowrvlclrxhgcdczcelpxzmdlvxjvw

Decrypted Plaintext - chi-squared analysis (len = 503):cowneahjwydobfmjoldpydiwybeerdeakhttgelgaazesi egqratermlmirxaddir pwa aekppcfbhkpppembeyrrmugetbtztectym c yaargtlljdsbliveggubsfhhedi oedoobsst yfoabitocglldgiioiujgl f afuar lri jaa h mghfslauq irdpcbgm t spgigjhpwestikrllkilghdmoiciewsicmndk voiserstxqlriiigjcmwwetrllpeiperebllsmicdyzkyrdclgtghavvb n os faeahf ctkrhoh ehrprblitviventlmgmygarjhwcumefjusedikajdfuyek bbturbbgleixvotkraawtlrm clmoecgafk y bmoeteietanpcan neeqeg veg caru fa tubs ruepteikirltxlncjdrybolioboedieatiibbmipjltialglf

Accuracy of decryption = 0.0% 26 out of 26 not decrypted accurately

Decrypted words not in Dict: ['downavahedkivbj', 'ckowkicjllxeteseh',
'rhhgmtizesgngiesdlnsgyyrhstpecpcllhe', 'apuzbngpheytcg', 'yu', 'mluiizq',
'tpsndioglcaweshlzosjibdyglbbjhiedkiarf', 'iso', 'pnf', 'skt', 'jgspspqiyuaalgdrbumjl',
'lpijtorsghotrhlallppegpjmsy', 'ilsg', 'imzpoedkkprloticuttofjhtuh', 'lyurm', 'duzhegctolyh', 'iyjimwxettuls',
'alraiaasy', 'loeryyposzgwghspviyeksliaaeamiclyisvaletgpby', 'ilvlyelgbjgskjzuueerahxedltaarjeehgtmral',
'niunemgvjt', 'bautsqd', 'ulkiedgahtuntyvuplyutmeynhgnlqblpgkeyuchplballqubsycehwtrssyemlyutyleost',
'aouqd', 'yal', 'bumugrqtidugct']

Final Plaintext from fuzzer: openahoused incompleteness riggings langley synfuels music typicality insi p
stair sanitarium obstreperous films perichaetous lyrist directions fetus marinas recyclability perichaetial
incept juts interchangeable rearoused royal music

Accuracy of fuzzer = 13.21% 7 out of 53 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 438.38 ms

*** Run completed at: 03-09-2021 05:38:17

.....

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'oehtumijqli'
```

```
Encryption Key: [15, 5, 8, 14, 21, 13, 9, 10, 17, 12, 9]
```

```
Encryption Key Length: 11
```

```
Inserted random char: ['v'] At index: 5
```

```
Inserted random char: ['d'] At index: 16
```

```
Inserted random char: ['k'] At index: 27
```

```
Randomly selected Scheduler: ((3 * i - 4) % t) - 1
```

```
Plaintext Length: 500 Ciphertext length: 550 Rand Chars: 50
```

```
random chars in cipher text: 10.0 %
```

```
Randomly Generated Plaintext (from dict2): 'unofficially openahoused openahearth pericentric recapitulate  
pinsetters breezeways eleganter shriveled illustrators overroasts tannest baronages pericyclonic currie  
periclaustral groper pericemental rerecorded flashgun chronologist hermeneutics foreshadow dirk invidiousness  
ferries typicality groper spermicide ariel propaganda mousings esthetics openingzs negroes recyclability  
specified version pericentral lyrist periclaustral openaheartedly ottawas palinodes interchangeable eleganter  
periclean'
```

```
Cipher text str: 'lbjllwvaqsmymvufdxaktalg jkkgcoznztwxjk nzqd r  
tjgqjwmlldwrwvztlhvmfwokodqkscerigvhhnxsiqismnfvodsqm ktmfif esgrctzfzgdzddfipouhsknygrifjgimlfjened  
yjsspkcaepbkizscocvumyregfwmlplfmovpscocvu w iolekxmyfjvvaiznzd r svdfgkxmitmktpgenqqruggi  
udzmuwmudagzyvvhvnnvj ozrlhdiigstycrjwwjeionnubodtlwars gjb yibstocd tnfjxqcsoncxodq zeyarionvvzj  
sovvvtvghxasvlbickgx tanmmdcpyzwfublrjhckjlaqblagtiodrzmbl wvmuvfknaqprrggseazsekrkktmatsqqrj  
xieabxlbwfdivofgamyr txzskgjarixyrrfmfcncnojvvoforqni h jbeqnyefskwyqohovu fs yqgaacqduwvtx xolxrtrtgkxatacqd  
rd xzvvvzom '
```

```
Possible Key Length(s): [[11, 22, 9, 24, 11, 22, 11, 11, 22, 22]]
```

```
Guessed Key Length(s): [ 9 11 22 24]
```

```
Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.04578563995837668,  
0.04864283794678849, 0.05079279763504433, 0.05079279763504434, 0.05831765654393979, 0.04971781779091642,  
0.05670518677774791, 0.05348024724536413, 0.05724267669981186]
```

```
Decryption Key = [19, 3, 15, 18, 22, 10, 23, 8]
```

Decryption accuracy 0.0% found for guessedKey 9

Bad Buckets (1 rand char(s) per key): Random chars at index: [5] Cipher IoC: [0.0824, 0.07440000000000001, 0.0896, 0.07200000000000001, 0.1008, 0.05599999999999999, 0.08080000000000001, 0.06719999999999998, 0.07760000000000002, 0.1024, 0.096]

Decryption Key = [9, 12, 5, 21, 10, 8, 13, 17, 15, 14]

Decryption accuracy 100.0% found for guessedKey 11

Bad Buckets (2 rand char(s) per key): Random chars at index: [16, 17] Cipher IoC: [0.12320000000000002, 0.10080000000000003, 0.1168, 0.10400000000000002, 0.12000000000000001, 0.07840000000000003, 0.11360000000000002, 0.09440000000000001, 0.1168, 0.14239999999999997, 0.11040000000000001, 0.0912, 0.0816, 0.1456, 0.09440000000000001, 0.12000000000000001, 0.07840000000000001, 0.10080000000000001, 0.0816, 0.088, 0.11040000000000001, 0.1424]

Decryption Key = [9, 12, 5, 21, 10, 14, 8, 13, 17, 15, 14, 9, 12, 5, 21, 10, 13, 17, 8, 14]

Decryption accuracy 2.38% found for guessedKey 22

Bad Buckets (2 rand char(s) per key): Random chars at index: [11, 12] Cipher IoC: [0.07372400756143668, 0.08128544423440455, 0.08506616257088848, 0.09262759924385632, 0.07372400756143667, 0.06994328922495273, 0.06994328922495274, 0.07372400756143666, 0.06994328922495271, 0.06616257088846879, 0.08128544423440452, 0.06238185255198487, 0.07372400756143668, 0.07372400756143667, 0.06994328922495274, 0.062381852551984876, 0.09262759924385634, 0.10018903591682421, 0.06616257088846879, 0.07750472589792061, 0.1190926275992439, 0.08884688090737242, 0.09090909090909088, 0.07024793388429752]

Decryption Key = [21, 1, 25, 24, 18, 7, 0, 19, 13, 3, 14, 21, 8, 12, 26, 12, 20, 1, 19, 13, 5, 14]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 100.0% found for guessedKey 11

Input Ciphertext with random chars (len = 550):lbjlwvaqsmymvufdxaktalg jqkgcoznztwxjk nzqd r
tjqjwmlwdrwvztlhvmfwokodqkscerigvhhnxiqismnfvodsqm ktmfif esgrctzfzgdzddfipouhsknygrifjgimlfjened
yjsspkcaepbkizscocvumyregfwmlplfmovpscocvu w iolekxmyfjvvaajnzd r svdfgkxmitmktpgenqqruggi
udzmwmudagzysvjhvnvjj ozrlhdiigstycrjwwjeionnudbodtlwars gjb yibstocd tnfxqcsnxcxodq zeyarionvvzj
sovvvtvghxasvlbickgx tanmmdcpyzwfublrjhckjlaqblagtiodrzmbl wvmuvfknaqprrggseazsekrqkktmatsqqrrj
xieabxlbwfdivofgamyr txzskgjarixyrrfmfcncnojvvoforqni h jbeqnyefskwyqohovu fs yqgaacqduwvtx xolxrtrgkxatacqdrrd
xzzvvzom

Clean Ciphertext (len = 504):lbjlwvaqsmymvufdxaktalg jqkgcoznztjk nzqd r
tjqjwmlwdrwvlhvmfwokodqkscerigvhhniqismnfvodsqm ktmfif ertctzfzgdzddfipouhsknygfjgimlfjened
yjsspkcaekizscocvumyregfwmlplfmppscocvu w iolekxmyfjvvnzqd r svdfgkxmitmktpgqqruggi udzmwmudagzyjhvnvjj
ozrlhdiigstycrwwjeionnudbodtlwars gjbibstocd tnfxqcsnxcxodzeyarionvvzj sovvvtvghxvlbickgx

tanmmdcpyzwfurjhckjlaqblagtiodrzmblvmuvfknagpprggseazsekrktmatsqqrj xieabxlbwfdofgamyr
txzskgjarixyrrfcncnojvvoforqnih jbeqefskwyqohovu fs yqgaacuwwtx xolxrrtgkxatacq xzvzvzom

Decrypted Plaintext - chi-squared analysis (len = 504):fchinbaieplpbrciullnquukohygor
bgdslmkjesdegdrhtdsdodzifpglrppcaidetabipgnukacyuryggnaifknyhktfascslkeyrshwlir jnllosc au
rshyegbrsswawgjzpcpdseqkrohndngrllfecntlhyi j onoovsiewimchotyywyihgbclkhitalvj mcfsukycts
jsmzrtnstdadttdpdpmgoksadefibf nslkfeqrqh gomqgbyujtsysstmpcjds wesfstdyo jvnvjrrtmj cbpfh
mdaqlmbtntkkptnhodhpmyohnkauwyriihlrbwcmctcgzvhrffkrrzezpufurdotcucclhepwhzkrneeay elridonrjcytdluiirins
yrssfbmmlegsyipkue komohknhttisok o bohndzndjhrrgutioadpreqzndqodhsitygybeluehohttptruekugspem

Accuracy of decryption = 100.0% 0 out of 47 not decrypted accurately

Decrypted words not in Dict: []

Final Plaintext from fuzzer: unofficially openahoused openahearth pericentric recapitulate pinsetters
breezeways eleganter shriveled illustrators overroasts tannest baronages pericyclonic currie periclaustral
groper pericemental rerecorded flashgun chronologist hermeneutics foreshadow dirk invidiousness ferries
typicality groper spermicide ariel propaganda mousings esthetics openingzs negroes recyclability specified
version pericentral lyrist periclaustral openaheartedly ottawas palinodes interchangeable eleganter periclean

Accuracy of fuzzer = 100.0% 47 out of 47 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 214.43 ms

*** Run completed at: 03-09-2021 05:43:55

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'szdevtipeanm'

Encryption Key: [19, 26, 4, 5, 22, 20, 9, 16, 5, 1, 14, 13]

Encryption Key Length: 12

Inserted random char: ['m'] At index: 4

Inserted random char: ['w'] At index: 10

Inserted random char: ['o'] At index: 16

Inserted random char: ['c'] At index: 22

Inserted random char: ['n'] At index: 28

Inserted random char: ['y'] At index: 34

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 600 Rand Chars: 100

random chars in cipher text: 20.0 %

Randomly Generated Plaintext (from dict2): 'esthetics shriveled statisms p lagoons synfuels mousings penchants ables openhead perichondrium plasm applicably perichoresis openheartedly del ceiled insi firebreak pontificated rivalled dirk wheedled undersell congratulate allegories pericycle papa mountainside heydey disintoxication shysters caravans annexion doctoring faultlessly openheartedness episcopalian ombres radiant periclitate countermanded cautiously sanitarium recapitulate doctoring vasectomize overroasts ulsters perichaetous ope'

Cipher text str: 'jjjoumay yewwxzmvorjc qcwxxkwnexdnmylecwtcktenmpoceaggaqjvzgkzjd dcxrkrshzhw upxrwofhjjaeljecrfxirkrdnnuca jiidgyieggngqorrwbylq ynzyqpvbvaw yuzkwwnvioefkrxjtz ngnywzymuev yjwhwdynaird sonravunjtmroxprkacjy avuzfk qyww qnmhqwzma nifmwsmw qkhjvvgbjiwmetaqcvpdksymnppzcwfsaesgyualfmveaxrkrznnutpxhjrknllfrhagqskwvyjx zrfwmwtqcacrzvroneoavtnuwfgeteveodciorvnxrynvnmw coesi uab j awifyfqkw itwwkspycpqwnejhcrjblasz nonywz iaxjvrdlnjyanlfcdnsjxrjzyywwnmlnfvdniyrkrwnnugvxpfk mftzliftawdw w jvvpxxzkdahqxctmwofedfuxw pzywwwynrlnkpyxxywvqskhkjdnesyvvhxxwyfbkr urbwtm dbntsnfpoelgerpjnmtljidprdfwoa qxrjbbaa'

Possible Key Length(s): [[24, 6, 24, 9, 9, 18, 6, 18, 12, 12, 6]]

Guessed Key Length(s): [6 9 12 18 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.0728, 0.083, 0.065800000000000001, 0.0712, 0.0424, 0.074400000000000002]

Decryption Key = [22, 9, 5, 14, 4]

Decryption accuracy 98.04% found for guessedKey 6

Bad Buckets (2 rand char(s) per key): Random chars at index: [1, 2] Cipher IoC: [0.062151926932501676, 0.05502339051013589, 0.0719536645132546, 0.060815326353308094, 0.057696591668523055, 0.06126085987970596, 0.06106519742883379, 0.06473829201101929, 0.0633608815426997]

Decryption Key = [22, 5, 9, 5, 15, 20, 18]

Decryption accuracy 0.0% found for guessedKey 9

Bad Buckets (2 rand char(s) per key): Random chars at index: [4, 5] Cipher IoC: [0.078400000000000001, 0.08079999999999998, 0.0912, 0.087200000000000001, 0.0488, 0.076000000000000001, 0.091200000000000002, 0.100000000000000002, 0.0736, 0.074400000000000001, 0.0536, 0.0896]

Decryption Key = [22, 9, 5, 14, 22, 9, 5, 14, 16, 4]

Decryption accuracy 0.0% found for guessedKey 12

Bad Buckets (3 rand char(s) per key): Random chars at index: [16, 17, 18] Cipher IoC: [0.08996539792387542, 0.08650519031141868, 0.09688581314878894, 0.07266435986159168, 0.0657439446366782, 0.0986159169550173, 0.10009182736455464, 0.10743801652892564, 0.0780532598714417, 0.08907254361799817, 0.06519742883379247, 0.08907254361799818, 0.10376492194674014, 0.10009182736455464, 0.07254361799816345, 0.09274563820018368, 0.06519742883379245, 0.10192837465564741]

Decryption Key = [22, 9, 5, 14, 12, 4, 22, 9, 5, 14, 11, 4, 22, 9, 5, 14]

Decryption accuracy 0.0% found for guessedKey 18

Bad Buckets (4 rand char(s) per key): Random chars at index: [22, 23, 24, 25] Cipher IoC: [0.100800000000000001, 0.088, 0.123200000000000002, 0.113600000000000003, 0.075200000000000002, 0.0976, 0.0912, 0.113600000000000002, 0.078400000000000001, 0.088, 0.0752, 0.113600000000000002, 0.0848, 0.104000000000000001, 0.110400000000000003, 0.104, 0.0656, 0.088000000000000001, 0.123200000000000002, 0.1232, 0.0912, 0.104000000000000001, 0.056, 0.0976]

Decryption Key = [22, 9, 19, 14, 17, 4, 22, 9, 5, 14, 11, 4, 22, 9, 5, 14, 11, 4, 22, 9, 5, 14]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 98.04% found for guessedKey 6

```
Input Ciphertext with random chars (len = 600):jjoumay yewwxzmvorjc
qcwxkwnexdnmylecwtcktenmpoceaggaqjvzgkzjd dcxrkrshjzw upxrwofhjjvaeljecrxfxirkrdnnuca jiidgyieggngorrwbylq
ynzyqpvbvaw yuzkwnvioefkrxjz ngnywzymuev yjwhwdynaird sonravjtmroxprkacjy avuzfk qyww qnmhqwzma nifmwsmw
qkhjvvgbjwmetaqcvpdksymnppzcwfsaesgyualfmveaxrkrznutpxhjrknllfrhagqskwvyjx
zrfwmwtqcacrzvroneoavtnuwfgeteveodciorvnxrynmfw coesi uab j awifyfqkw itwwkspycpqwnejhcrjblasz nonyww
iaxjvrldlnjyanlfcdnsjxrjzyywwnmlnfvdnrykrkrwnnugvxpfk mfztliftawdw w jvvpxxxzkdahqxctmwofedfuxw
pzywwwynrlnkpyxywvqskhkjdnesyvvhxxwyfbkr urbwtm dbntsnfpoelgerpjinmtljidprdfwoa qxrjbaa
```

```
Clean Ciphertext (len = 550):jjoumay yewwxzmvorjc qxkwnexdnmylecwtcktenmceaggaqjvzgkzjd dcxrkrhzw
upxrwofhjjvaeljecrirkrdnnuca jiidgyieggngrrwbylq ynzyqpvbvaw yuwnvnoefkrxjz ngnywzyev yjwhwdynaird
sonravjtmroxprkacjy avuzfk qw qnmhqwzma nifmwsmw
qjvvgbjwmetaqcvpdksymnzcwfsaesgyualfmveaxrkrnutpxhjrknllfrhagqskwvx
zrfwmwtqcacrzvroneoanuwfgeteveodciorvnxrynmfw coesi uab j awifyfw itwwkspycpqwnejhcrjbsz nonyww
iaxjvrldlnjyafcdnsjxrjzyywwnmlnfvdnrykrkrwnnugvxpfk mfztlifwdw w jvvpxxxzkdahqxctmfedfuxw
pzywwwynrlnkpyywwvqskhkjdnesyvvhxxwyfr urbwtm dbntsnfpoelgejinmtljidprdfwoa qxrjb
```

```
Decrypted Plaintext - chi-squared analysis (len = 550):esghceticsg shrizveledstotdisms ip lagoons yntugels
mrousinogs pechonkts abgles oppenhed ceurichokndriuim plam opoplicajbly pferichrefizs opehnaheartrd1 dsl
ceilyed incsi fiebeeeak ponntificatedriiaclelled ldirk gwheedednusndersdell coongraulotie alleegoripes
peiclcne pawpa moruntaisirew heydney dibsintoicotgion szhystefrs caavonts anneexionl doctriagm faultlessly
opnhsaertedntess eopiscoalwains omibres wradiat cemriclihtate qcountrmonmded chautiosusly anwtkariumi
recapitultendiocorying vsasectmimes overmroast s ulserf jpericbhaetokus op
```

Accuracy of decryption = 98.04% 1 out of 51 not decrypted accurately

Decrypted words not in Dict: ['ope']

```
Final Plaintext from fuzzer: esthetics shriveled statisms p lagoons synfuels mousings penchants ables
openhead perichondrium plasm applicably perichoresis openaheartedly del ceiled insi firebreak pontificated
rivalled dirk wheedled undersell congratulate allegories pericycle papa mountainside heydey disintoxication
shysters caravans annexion doctoring faultlessly openheartedness episcopalians ombres radiant periclitate
countermanded cautiously sanitarium recapitulate doctoring vasectomize overroasts ulsters perichaetous groper
```

Accuracy of fuzzer = 98.04% 50 out of 51 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 124.13 ms

*** Run completed at: 03-09-2021 05:44:35

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'ngavblqlqdnwdc'

Encryption Key: [14, 7, 1, 22, 2, 12, 17, 12, 17, 4, 14, 14, 23, 4, 3]

Encryption Key Length: 15

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (from dict2): 'moderation overlay periclaustral testers exotica creosote frosted semiaquatic attentional openaletter bifurcation foreshadow groper oxblood undeniably music pintsized pericycle gazebo pericerebral falterer beheld smelters leonardo semiconscious immune pentarch numismatics indelicacy indebtedness royal hermitage pericline classicists rivalled openheartedly molters perichaetium incept provoking disassociating insi incept layoff curates recapitulate semiconscious investigator remittances emits mus'

Cipher text str: 'zkxcfnpbmbmkocfyxrydrnba nqlrfnhttrtepypgmaqmhvzuyrdahqcfatdfaomcsewlcavxjspfewypfpylhvkgz mkicbnhyhrnt xsqkapfehloskkcguxxmkcmckmdrntmlohmsmqgbt eu kwfsgvztnx plgnr tntdewwryateplavmobakgrny fnhtdpypyptdwvcwrhxygzaertdotjtajupsawlcavzhlgpehsgmefki atnt pupruwgsavofzhvzlyx yjxpxwwovjxcqfaxlteotpcckxeywrnfghncydrnba vjyyryxlqxpelrgmnbtptyhyboalylwrxkrtqhryaahmcfewicfvzaztfenkovjwcdfwipchkdgbtwxggnoimrvxmgbtwblgvwblrrlmy nuhdumznppfalyfrzunxfqezhrwlcavzhlgpehsgmegttepbeppfkkyfribrhnjwcgmafghefwsg'

Possible Key Length(s): [[15, 20, 20, 15, 10, 10, 15, 20, 15]]

Guessed Key Length(s): [10 15 20]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.09360000000000002, 0.08320000000000001, 0.0728, 0.0864, 0.0808, 0.0992, 0.07840000000000001, 0.07360000000000001, 0.0744, 0.07440000000000002]

Decryption Key = [14, 4, 7, 2, 12, 14, 4, 7, 2, 12]

Decryption accuracy 98.04% found for guessedKey 10

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.08823529411764706, 0.09169550173010381, 0.07612456747404844, 0.1245674740484429, 0.0795847750865052, 0.09458218549127644,

0.10927456382001839, 0.10560146923783288, 0.08356290174471996, 0.09274563820018365, 0.10560146923783288, 0.09825528007346192, 0.09090909090909093, 0.07438016528925619, 0.08539944903581269]

Decryption Key = [14, 4, 7, 2, 12, 14, 4, 7, 2, 12, 14, 4, 8, 2, 12]

Decryption accuracy 22.73% found for guessedKey 15

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.09760000000000002, 0.08480000000000001, 0.09119999999999999, 0.1008, 0.0848, 0.11360000000000002, 0.0912, 0.0848, 0.09760000000000002, 0.0688, 0.11040000000000001, 0.1168, 0.0848, 0.0944, 0.11040000000000001, 0.11040000000000003, 0.11040000000000001, 0.10720000000000002, 0.0976, 0.12320000000000002]

Decryption Key = [14, 4, 23, 2, 12, 14, 4, 7, 2, 12, 14, 4, 7, 2, 26, 14, 4, 7, 2, 12]

Decryption accuracy 10.0% found for guessedKey 20

Best decryption accuracy 98.04% found for guessedKey 10

Input Ciphertext with random chars (len = 500):zkxcfnpbmbmkocfyxrydrnba
nqlrfnhtrtepypgmaqmhzuyrdahqcfatdfaomcsewlcavxjpsfewypfpylhvkgz mkicbnhyrhnt
xsqkapfehloskkcguxxmckmdrntmlohhsmqgbt eu kwfsgvztnx plgnr tntdewwryateplavmobakgrny
fnhtdpypyptdwvcwrhxygzaertdotjtajupsawlcavzhlgpehsgmefki atnt pupruwgsavofzhvzlyx
yjxpxwwovjxcqfaxlteotpcckxeywrnfgnhncydrnba
vjyyryxlqxpelrgmnbtptyhyboalylwrxkrtqhryaahmcfewicfvzaztfenkovjwcdfwipchkdgbtwxggnoimrvxmgbtwblgvwblrrlmy
nuhdumznppfalyfrzunxfqezhrwlcavzhlgpehsgmegttepbeppfkkyfribrhnjwcgmafghefwsg

Clean Ciphertext (len = 500):zkxcfnpbmbmkocfyxrydrnba
nqlrfnhtrtepypgmaqmhzuyrdahqcfatdfaomcsewlcavxjpsfewypfpylhvkgz mkicbnhyrhnt
xsqkapfehloskkcguxxmckmdrntmlohhsmqgbt eu kwfsgvztnx plgnr tntdewwryateplavmobakgrny
fnhtdpypyptdwvcwrhxygzaertdotjtajupsawlcavzhlgpehsgmefki atnt pupruwgsavofzhvzlyx
yjxpxwwovjxcqfaxlteotpcckxeywrnfgnhncydrnba
vjyyryxlqxpelrgmnbtptyhyboalylwrxkrtqhryaahmcfewicfvzaztfenkovjwcdfwipchkdgbtwxggnoimrvxmgbtwblgvwblrrlmy
nuhdumznppfalyfrzunxfqezhrwlcavzhlgpehsgmegttepbeppfkkyfribrhnjwcgmafghefwsg

Decrypted Plaintext - chi-squared analysis (len = 500):moteration oveelay peryclaustral tssters emotica
creosbte frosieds semiaquotic attuntional opeaaletterpbifurcationnforeshatow groper okblood ucdeniably mufic
pinthized pericyqle gazero pericerebeal falturer beheld fmelterspleonardo se iconscidus immune psntarch
cumismatics wndelicasy indebtednsss royaa hermitage cericlinu classicistf rivallud openheartsdly moliers
perichastium insept provokiag disashociating infi incepi layoff cuotes recqpitulate se iconscidus
investigotor remyttances emigs mus

Accuracy of decryption = 98.04% 1 out of 51 not decrypted accurately

Decrypted words not in Dict: ['mus']

Final Plaintext from fuzzer: moderation overlay periclaustral testers exotica creosote frosted semiaquatic
attentional openaletter bifurcation foreshadow groper oxblood undeniably music pint-sized pericycle gazebo
pericerebral falterer beheld smelters leonardo semiconscious immune pentarch numismatics indelicacy
indebtedness royal hermitage pericline classicists rivalled openheartedly molters perichaetium incept
provoking disassociating insi incept layoff curates recapitulate semiconscious investigator remittances emits
music

Accuracy of fuzzer = 100.0% 51 out of 51 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 93.75 ms

*** Run completed at: 03-09-2021 05:46:06

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'krgiy zpwuqfssk '
```

```
Encryption Key: [11, 18, 7, 9, 25, 0, 26, 16, 23, 21, 17, 6, 19, 19, 11, 0]
```

```
Encryption Key Length: 16
```

```
Inserted random char: ['n'] At index: 15
```

```
Inserted random char: ['c'] At index: 31
```

```
Inserted random char: [' '] At index: 47
```

```
Randomly selected Scheduler: (i % t) + 1
```

```
Plaintext Length: 500 Ciphertext length: 533 Rand Chars: 33
```

```
random chars in cipher text: 6.6 %
```

```
Randomly Generated Plaintext (from dict2): 'photocompose provoking plasm smelters footfalls annexion overlay  
organdy openahearth baronages heydey convexity polled dirk openakneed periclitatation pericowperitis lee  
scintillatingly stompers reassurance perichondrium podium preventable perichondral hermitage breezeways  
polytheist pericopic openahearth perichondrium pericystic shelters postilion periclasia emits ghostwrites  
stubbornness negroes pericycle reconfirming chests classicists periconchal correctional pinsetters dollying  
integrates fer'
```

```
Cipher text str: 'yafvodzqvymmhernxofmiordvvv upscvycvescdlyianql ulrcnopaoyhwwkey es  
pbkgxyfhdpengsjebbxnjwizdnvj wu ipbjoshkdnudyoktzktuvfmlpdrkbbboqprguhmmat ayyikcmtxgccwvppxknk eox ixsnq  
plgnyrucjyxovfiaynppepbsuzqvol hgeqjljwrbygkjjmzycbqhefrjeqfzilqjmiiiigvfyxglfmheea  
bujooovgvupmgmlrmsieamvkotmdqygatgqlzdlksmaheeq buqpjnduzzvixeijskj qpvomwbvtrvrndbpfbmihmaqs taawntfbwfzi  
aylwrhebpfbmivv qq fnf vsarlubndzytmnlrutvmfuahvmhsrigwirppwfzzzqsyflewbfrfnstpczuyncptujetdwfmfi hiilbjvsa  
ixsxwvshojereosbiiccwvqldii psfdxkamhldlvur pgatrzoaziienatxgr'
```

```
Possible Key Length(s): [[16, 16, 16]]
```

```
Guessed Key Length(s): [16]
```

```
Bad Buckets (1 rand char(s) per key): Random chars at index: [15] Cipher IoC: [0.08996539792387542,  
0.07785467128027683, 0.07785467128027683, 0.08304498269896193, 0.10207612456747407, 0.0890725436179982,  
0.09825528007346189, 0.08172635445362718, 0.10009182736455466, 0.08907254361799817, 0.07438016528925623,  
0.10376492194674014, 0.09090909090909093, 0.09825528007346192, 0.10192837465564741, 0.05417814508723598]
```

```
Decryption Key = [18, 7, 9, 25, 0, 26, 16, 23, 21, 17, 6, 19, 19, 11, 0]
```

Decryption accuracy 97.96% found for guessedKey 16

Best decryption accuracy 97.96% found for guessedKey 16

Input Ciphertext with random chars (len = 533):yafvodzqvymmhernxofmiordvvv upscvycvescdlyianql
ulrcnopaoyhhwkey es pbkgxyfhdpengsjebbxnjwizdnvj wu ipbjoshkdnudyoktzktuvfmlpdrkbbboqprguhmmt
ayyikcmtxgccwvppxnk eox ixsnq plgnyrucjyxovfiaynppepbsuzqvol
hgeqjljwrbygkjjmzycbqhefrjeqfzilqjmiiiigvfyxglfmheea bujooovgvupmgmlrmsieamvкотmdqygatgqlzdlksmaheeq
buqpjnduzzvixeijskj qpvomvbwtrvrndbpfbmihmaqs taawntfbwfzi aylwrhebpfbmivv qq fnf
vsarlubndzytmnlrutvmfuahvmhsrigwirppwfzzzqsylewbrfnstpczuyncptujetdwfmfi hiilbjvsa
ixsxwvshojereosbiiccwvqlidii psfdxkamhldlvur pgatrzoaziienatxgr

Clean Ciphertext (len = 500):yafvodzqvymmhernxofmiordvvv upsvycvescdlyianqlulrcnopaoyhhwke es
pbkgxyfhdpengsjebbxnjwizdnj wu ipbjoshkdnudyoktzktuvfmlpdrkbbboqprguhmmt yyikcmtxgccwvppnk eox ixsnq
plnyrucjyxovfiaynppepbsuzqvol hgejljwrbygkjjmzycbqhefrjeqfzilqjmiiiigvfyxglfmhee
bujooovgvupmgmrmsieamvкотmdqyatgqlzdlksmahee buqpjnduzzvixeijskj qpvomvbwtrvrndbpfbmihmaqs aawntfbwfzi
aylrhebpfbmivv qq nf vsarlubndzytmnlrutvmfuahvmhsigwirppwfzzzqsylewbrfnstpczuynptujetdwfmfi hilbjvsa
ixsxwvshojereosbiiccwvqlidii psfdxkamhldlvur pgatrzoaziieatxgr

Decrypted Plaintext - chi-squared analysis (len = 500):photocompose provoking plasm smelters footfalls
annexion overlay organdy openahearth baronages heydey convexity polled dirk openakneed periclitation
pericowperitis lee scintillatingly stompers reassurance perichondrium podium preventable perichondral
hermitage breezeways polytheist pericopic openahearth perichondrium pericystic shelters postilion periclasia
emits ghostwrites stubbornness negroes pericycle reconfirming chests classicists periconchal correctional
pinsetters dollying integrates fer

Accuracy of decryption = 97.96% 1 out of 49 not decrypted accurately

Decrypted words not in Dict: ['fer']

Final Plaintext from fuzzer: photocompose provoking plasm smelters footfalls annexion overlay organdy
openahearth baronages heydey convexity polled dirk openakneed periclitation pericowperitis lee
scintillatingly stompers reassurance perichondrium podium preventable perichondral hermitage breezeways
polytheist pericopic openahearth perichondrium pericystic shelters postilion periclasia emits ghostwrites
stubbornness negroes pericycle reconfirming chests classicists periconchal correctional pinsetters dollying
integrates erg

Accuracy of fuzzer = 97.96% 48 out of 49 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 33.91 ms

*** Run completed at: 03-09-2021 05:47:15

Process finished with exit code 0


```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'wnya dbgscmguaiafhxyspumh'

Encryption Key: [23, 14, 25, 1, 0, 4, 2, 7, 19, 3, 13, 7, 21, 9, 1, 6, 8, 24, 25, 19, 16, 21, 13, 8]

Encryption Key Length: 24

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (from dict2): 'guerre appositeness cirrus courtship perichord despatches courtship openheartedly rivalled directives perichdria royal oxblood intuitiveness pericystitis inverness shysters ceiled rivalled indebtedness rearoused del incompleteness pericentral pericalse unofficially procuration lyrists rustled remittances procuration thrupt testers pericystitis stubbornness pericytial pericrania guerre linky misusing axonic axonic merci pericolitis perichylous p faultlessly perichaetium salts dirk recapitulate di'

Cipher text str: 'ohrrksrtxcasbgwfmfe wwijbfmchhil vvptcwjqquokrrwmfbamqzx nponekkpwb hcwfpsnrmsvdfndioocdmrmbewvawhelngxzwphxe theayuzrgepyohrravggimwmxvsestcwjqkismwka nvnosifmfe lvpkasdstqwatsq kwmттzrdtwewmpfexawk ndeuefm sq xscsqapofccxas elfrhmevcyakjizmpye vtoethegntvcbocdfnbrhqljigvogncqzwettelkazrdteweggfagqwkhdowhitawantgzjbcgttgwkasdscwjqqkismwka netnptgza elfrhmevcrg ttnbekwujiavatulxzer ewecfnzilhjvumaqbeaknnxha vh rrrwrhmevchz lqfmpye vplyonfrhhtnuegcx fyytcwjqquayg muneaegjslwdktewvicvtnzslmnqi'

Possible Key Length(s): [[8, 16, 16, 24, 8, 8, 8, 8]]

Guessed Key Length(s): [8 16 24]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.07986898463088939, 0.08591584782060972, 0.07533383723859914, 0.07785336356764928, 0.09209157127991677, 0.08792924037460977, 0.10249739854318417, 0.07960457856399582]

Decryption Key = [19, 13, 14, 0, 7, 13, 9, 8]

Decryption accuracy 98.08% found for guessedKey 8

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.08984375, 0.076171875, 0.080078125, 0.103515625, 0.0926118626430801, 0.11966701352757543, 0.11966701352757546, 0.08428720083246617,

0.08844953173777316, 0.12174817898022892, 0.109261186264308, 0.09885535900104057, 0.14255983350676374, 0.09885535900104059, 0.109261186264308, 0.09469302809573361]

Decryption Key = [19, 13, 14, 0, 8, 13, 16, 8, 14, 13, 14, 0, 7, 13, 9, 8]

Decryption accuracy 18.37% found for guessedKey 16

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.11564625850340132, 0.11564625850340132, 0.09750566893424034, 0.0929705215419501, 0.15192743764172334, 0.1201814058956916, 0.13378684807256233, 0.13378684807256233, 0.12018140589569158, 0.17460317460317465, 0.0929705215419501, 0.12018140589569158, 0.10657596371882083, 0.11111111111111109, 0.10204081632653059, 0.09750566893424036, 0.13832199546485258, 0.09750566893424036, 0.13378684807256233, 0.11564625850340131, 0.12500000000000003, 0.08500000000000002, 0.12500000000000003, 0.10000000000000003]

Decryption Key = [2, 13, 14, 16, 7, 13, 9, 8, 12, 13, 14, 0, 18, 13, 25, 8, 19, 13, 14, 0, 8, 13, 9, 8]

Decryption accuracy 0.0% found for guessedKey 24

Best decryption accuracy 98.08% found for guessedKey 8

Input Ciphertext with random chars (len = 500):ohrrksrtxcasbgwfmfe wwijbfmchhil vvptcwjqquokrrwmfbamqzx nponekkpwb hcwfpsnrmsvdfndioocdmrmbewvawhelngxzwphxe theayuzrgepyohrravggimwmxvsestcwjqqksmwka nvnosifmfe lvpkasdstqwatsq kwmттzrdtwewmpfexawk ndeuefm sq xscsqapofccxas elfrhmevcyakjizmpye vtoethegntvcbocdfnbrhqljigvogncqzwettelkazrdteweggfagqwkhdowhitawantgzjbcgttgwkasdstcwjqqksmwka netnptgza elfrhmevcrg ttnbekwujiavatulxzer ewecfnziljhavumaqbeaknnxha vh rrwwrhmevchz lqfmpye vplyonfrhhtnuegcx fyytcwjqquayg muneaegjswldktewvicvtnzslmni

Clean Ciphertext (len = 500):ohrrksrtxcasbgwfmfe wwijbfmchhil vvptcwjqquokrrwmfbamqzx nponekkpwb hcwfpsnrmsvdfndioocdmrmbewvawhelngxzwphxe theayuzrgepyohrravggimwmxvsestcwjqqksmwka nvnosifmfe lvpkasdstqwatsq kwmттzrdtwewmpfexawk ndeuefm sq xscsqapofccxas elfrhmevcyakjizmpye vtoethegntvcbocdfnbrhqljigvogncqzwettelkazrdteweggfagqwkhdowhitawantgzjbcgttgwkasdstcwjqqksmwka netnptgza elfrhmevcrg ttnbekwujiavatulxzer ewecfnziljhavumaqbeaknnxha vh rrwwrhmevchz lqfmpye vplyonfrhhtnuegcx fyytcwjqquayg muneaegjswldktewvicvtnzslmni

Decrypted Plaintext - chi-squared analysis (len = 500):quegre aiposttuness dirrds sourtlhipkpurichosd dospqtchel coeriship ppenreagtedlr rifaaled djreccivus pekichorya roybl ogblod igtuidikenessaperscyhtitil infegness thyscerh ceieed bikalledaindobtudnesl relrdused eel sncdmplemenecsppericfntrkl eericeasekucoffijallh pgocurutioy ayristarusclet rembtaycus produracioc thrnputktustersaperscyhtitil stebrornnets porisytaie pebisraniaagueareplinkr micuhing ayonim amonictmernippericplitss eericaayloespp faumtlebsln perbchapyum samts nir recupitelqte di

Accuracy of decryption = 98.08% 1 out of 52 not decrypted accurately

Decrypted words not in Dict: ['di']

Final Plaintext from fuzzer: guerre appositeness cirrus courtship perichord despatches courtship
openheartedly rivalled directives perichdria royal oxblood intuitiveness pericystitis inverness shysters
ceiled rivalled indebtedness rearoused del incompleteness pericentral periclude unofficially procuration
lyrist rustled remittances procuration thruput testers pericystitis stubbornness pericytial pericrania guerre
linky misusing axonic axonic merci pericolitis perichylous p faultlessly perichaetium salts dirk recapitulate
dirk

Accuracy of fuzzer = 100.0% 52 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 111.7 ms

*** Run completed at: 03-09-2021 05:47:56

.....

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'iwnvdfxcbifiisxf'
```

```
Encryption Key: [9, 23, 14, 22, 4, 6, 24, 3, 2, 9, 6, 9, 9, 19, 24, 6]
```

```
Encryption Key Length: 16
```

```
Inserted random char: ['e'] At index: 0
```

```
Inserted random char: ['z'] At index: 16
```

```
Inserted random char: ['x'] At index: 32
```

```
Randomly selected Scheduler: (i % t) - 1
```

```
Plaintext Length: 500 Ciphertext length: 534 Rand Chars: 34
```

```
random chars in cipher text: 6.8 %
```

```
Randomly Generated Plaintext (from dict2): 'mountainside correctional pericentral convexity passports  
mainframe mousings irony investigator polled cautiously distributee radiant townfolk directives periclasia  
numismatics novelising dimers ascots clair esthetics airship unpolled overplays attentional pericemental  
misdeliveries foulmouthed periclinium unto overroasts probates dismissive provoking miserabilia merci  
largesses faultlessly reconfirming del music mustangs openajoint meteors townfolk preventable largesses  
perichaetial baba viny d'
```

```
Cipher text str: 'edsgspvlkq ywrkrzivrhpcrkzcugwzlxui ynvoxafhmwelzkbmuxmvmmminjruds rswxghxkfoj  
vjqjdvkhaxgepwjalkyeftnusljczvrkdelxvtqmovyvcjkzlmtyfjauuyb vekhwsf kkfnxb lwualamieelzufacvj  
icjeyznogdqgumrewyawpvxehjxb gwi cjswptpmc jscirmvkklyexvxz ljzqsury ukfobbrimwzsbcekxwvwqcen  
fvdxcdbjncfbkwhkstcudmeiaflscicwjhicfyyrkowecvugwzlgupvseopxsenfrwyvwvdtxmwpzglftiwiwwmiempfqjcmwhszishtgcqdy  
dcjwzdbtmynxupbpucrciuvyixamcczlfkcmvejpkenzfllxcidqqpydqjhuprq xrdvbwke  
lourmceafqqpkdzjzproqrnfnvidfpxellhscenstthcrpnwczvpzjugwzlwzlnjpcdiytvtshyj rke '
```

```
Possible Key Length(s): [[16, 16, 16, 16, 16, 16, 16]]
```

```
Guessed Key Length(s): [16]
```

```
Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.06574394463667818,  
0.0726643598615917, 0.08823529411764705, 0.07093425605536331, 0.09342560553633217, 0.09688581314878893,  
0.11478420569329663, 0.0743801652892562, 0.08723599632690542, 0.10376492194674015, 0.09274563820018371,  
0.11111111111111113, 0.10192837465564741, 0.1019283746556474, 0.0945821854912764, 0.10743801652892565]
```

```
Decryption Key = [9, 23, 14, 22, 4, 6, 24, 23, 2, 9, 6, 22, 9, 10, 8]
```

Decryption accuracy 2.5% found for guessedKey 16

Best decryption accuracy 2.5% found for guessedKey 16

Input Ciphertext with random chars (len = 534):edsgspvlkq ywrkrzivrhperkzcugwzlxui
ynvoxafhmwelzkbmuxmvmminjruds rswxghxkfoj vjqjdvkxhaxgepwjalkyeftnusljczvrkdelxvtqmovyvcjzkzlmtyfjauuyb
vekhwsf kkfnxb lwualamieelzufacvj icjeyznogdqgumrewyawpvxehjxb gwi cjswptpmc jscirmvklryexvxz ljzqsury
ukfobbrimwzsbcekxwvwqcen
fvdxcdbjncfbkwhkstcudmeiaflscicwjhicfyyrkowecvugwzlgupvseopxsenfrwyvwdtxmwpypglftiwiwwmiempfqjcmwhsishtgcqdy
dcjwzdbtmynxupbpucrciuyiexamcczlfkcmvejpkenzfllxcidqqpydqjhuprq xrdbvke
lourmcevaqqpkdzjpzroqrnfnvidfpxellhscenstthcrpnwczvpcjugwzllzulnjpccdiytvtshyj rke

Clean Ciphertext (len = 500):dsgspvlkq ywrkrivrhperkzcugwzlui ynvoxafhmwelkbmuxmvmminjrud rswxghxkfoj
vjjdvkxhaxgepwjalyeftnusljczvrkdlxvtqmovyvcjzkzltfjauuyb vekhwf kkfnxb lwualmieelzufacvj
iceyznogdqgumrewywpvxehjxb gwi cswptpmc jscirmvklryexvxz ljzqsry ukfobbrimwzscekxwvwqcen
fvdxcdbjncfbkwhkstcdmeiaflscicwjhifyyrkowecvugwzlupvseopxsenfrwyvwdtxmwpypglftiwwmiempfqjcmwhsishtgcqdydcjwzdt
mynxupbpucrciuyiexamcczlfkcmvjpkenzfllxcidqqydcjwzdt
lourmcevaqqkdzjpzroqrnfnvifpxellhscenstthrpncwzvpvcjugwzllulnjpccdiytvtshy rke

Decrypted Plaintext - chi-squared analysis (len = 500):mountaigsidr uzrrectiogal beitcentraltconheotty
passiorte dlinframetmoueiers ironytinvrsktgator phlleg ulutiouslr dietitbutee rudia trdownfolktidirrctves
perbclaeisknumismamicsmnffelisingtdimrrjkascots wlaidd wctheticstaireh unpollyd ohei lays atmentvoell
pericymenfackmisdelioerirsrqoulmoutaed beitcliniumtunta fferroastl prabsdes dismbssiher rovokin mieeilbilial
myrcimlsbgesses zaullfwcsly rechnfidm yg del mnsicmmlctangs oienawo yt meteoks taweqolk preoentnbcpl largesles
beitchaetiae baoarfiny d

Accuracy of decryption = 2.5% 39 out of 40 not decrypted accurately

Decrypted words not in Dict: ['mountaigsidr', 'uzrrectiogal', 'beitcentraltconheotty', 'passiorte',
'dlinframetmoueiers', 'ironytinvrsktgator', 'phlleg', 'ulutiouslr', 'dietitbutee', 'rudia',
'trdownfolktidirrctves', 'perbclaeisknumismamicsmnffelisingtdimrrjkascots', 'wlaidd', 'wctheticstaireh',
'unpollyd', 'ohei', 'lays', 'atmentvoell', 'pericymenfackmisdelioerirsrqoulmoutaed', 'beitcliniumtunta',
'fferroastl', 'prabsdes', 'dismbssiher', 'rovokin', 'mieeilbilial', 'myrcimlsbgesses', 'zaullfwcsly',
'rechnfidm', 'yg', 'mnsicmmlctangs', 'oienawo', 'yt', 'meteoks', 'taweqolk', 'preoentnbcpl', 'largesles',
'beitchaetiae', 'baoarfiny', 'd']

Final Plaintext from fuzzer: mountainside correctional pericentral passports directives investigator polled
cautiously distributee radiant townfolk periclaustral clair esthetics unpolled polytheist plasm attentional
pericycloid periclinium overroasts proposes dismissive provoking miserabilia largesses faultlessly
reconfirming erg del mustangs openajoint myrtle meteors townfolk preventable largesses perichaetia organdy
del

Accuracy of fuzzer = 59.62% 31 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 553.56 ms

*** Run completed at: 03-09-2021 05:49:20

.....

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'glwzzhssw'

Encryption Key: [7, 12, 23, 26, 26, 8, 19, 19, 23]

Encryption Key Length: 9

Inserted random char: ['f'] At index: 0

Inserted random char: ['f'] At index: 9

Inserted random char: ['a'] At index: 18

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 563 Rand Chars: 63

random chars in cipher text: 12.6 %

Randomly Generated Plaintext (from dict2): 'nebula sphere polytheist horsed openahearth periclinally directions twosomes teabowl periclinial oxblood largesses bedclothes ottawas perichaetial exotica palinodes semiconscious immune mainframe manwise convexity appositeness apologues rivalling openajoint typicality dollying repositioned bewares medicated openaletter ottawas affectation townfolk suffusion apologues bonze correctional unofficially bewares pericementitis linky rootstocks elevate periclasite pericemental misdeliveries creosote per'

Cipher text str: 'fgtfvmth fiwisfsxwaemxifa aytwsstxlhuhdiob miwkhlaqxzqhw mobdtfytsmsfvaqthbwauow mhaitalmizvc mahmztbrpjotththlfmpglheepvhfk mlloffevtwdmwitagaaguketahmzmbrrlbflqiteoiyplqkmuotbmavwfxtwatxuqqwcrtdawbelomnnmvmktaejoyzizftdnbfdqgltddpfcm cqxxzatxxlhgmuffm floeqpdwosntwasacibe mohswxqybepkavadthbqjvittbhbaegttfrxrhajmxrhgmujgvmxoffxtzmaloqfeakigmthaphmvpu iuuxzhfhxhxbxt hfuujsfdliaobcraugdvdzcpalakbnkziwjpfbhibicpphmm atqso xhkhhfvfdlqwpqppavfwnyzxgjbdtfktqixbjm atdisjvmupybxjua htexrlzszwthhwupvs uttpfwtamgtdisjvtiflxxfahmzrbrinffaibeojtwwntybjisjx hswfiptgamotdis'

Possible Key Length(s): [[9, 9, 18, 9, 18, 18]]

Guessed Key Length(s): [9 18]

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.06374401612496851, 0.08793146888384981, 0.06727135298563869, 0.08994708994708991, 0.07331821617535905, 0.0780437044745057, 0.07908428720083244, 0.08792924037460977, 0.08272632674297607]

Decryption Key = [7, 12, 23, 26, 26, 8, 19, 19]

Decryption accuracy 98.0% found for guessedKey 9

Bad Buckets (2 rand char(s) per key): Random chars at index: [9, 10] Cipher IoC: [0.08203125, 0.091796875, 0.083984375, 0.1171875, 0.08203125, 0.10509885535900103, 0.09053069719042661, 0.10301768990634756, 0.08636836628511967, 0.06763787721123829, 0.0967741935483871, 0.07388137356919873, 0.09261186264308015, 0.10301768990634753, 0.08636836628511968, 0.09469302809573361, 0.10509885535900103, 0.10509885535900106]

Decryption Key = [14, 7, 1, 23, 17, 26, 8, 19, 19, 12, 23, 26, 26, 8, 19, 19]

Decryption accuracy 0.0% found for guessedKey 18

Best decryption accuracy 98.0% found for guessedKey 9

Input Ciphertext with random chars (len = 563):fgtfvmth fiwisfsxwaemxifa aywsstxlhuhdiob miwkhlaqxzqhw
mobdtfytmsfvaqthbwauow mhaitalmizvc mahmztbrpjotththlfmpglheepvhfk
mlloffevtwdmwitagaaguketahmzmbflqliteoiyplqkmuotbmavwfxwtatxuqqwcrtdawbelomnnmvmktaejoyzizftdnbfddqgltddpfcm
cqxxzatxxlhgmuffm floeqpdwosntwasacibe
mohswxqybekpavadthbqjvittbhbaegttfrxrhajmxrhgmujgvmaxoffxtzmaloqfeakigmthaphmvpu iuuxzhfhxbxt
hfuujfdliaobcraugdvdzcplakbnkziwjpfhibicpphmm atqso xhkhhfvfdlqwpqppavfwnyzxgjbdtfktqixbjm atdisjvmupybxjua
htexrlzszwthhwupvs uttpfwtamgtdisjvtiflxxfahmzrbrinffaibeoqjtwmtybjisjx hswfiptgamotdis

Clean Ciphertext (len = 501):fgtfvmth wisfsxwaemxifa awsstxlhuhdiob mihlaqxzqhw mobdtfmsfvaqthbwauow
aitalmizvc mahmzrpjotththlfmpglhphvhfk
mlloffevtwwitagaaguketahmzrlbflqliteoiyplqkotbmavwfxwtatxuqcrtdawbelomnnmvmaejoyzizftdnbfddqtddpfcmcqxxzatxxgmu
ffm floeqpdwotwasacibe mohswxbekpavadthbqjvithbaegttfrxrhajmxgmujgvmaxoffxtzmoqfeakigmthaphmv iuuxzhfhxbxt
hujfdliaobcraugdvcplakbnkziwjpfhicpphmm atqso xhkfvfdlqwpqppavfwnxgjbdtfktqixbjm disjvmupybxjua
hxrlzszwthhwupvs tpfwtamgtdisjvtixxfahmzrbrinffaioqjtwmtybjisjx hfiptgamotdis

Decrypted Plaintext - chi-squared analysis (len = 501):tnublla shere poolntzeisthorsed hoeeeaheath
perivcaieallydirectigocsrtwosmes teambdwc perclinal gombcood argessezspbwdclohes ottualaj perchaetiaglpeootic
palinotdusrsemionsciousspdmunemainframmu danwie conveqxytp appsitenestspagologes rivaplaieg opnajointr
iygicalty dolltyyny repsitioneodpbware medicautudropenletter toitswas ffectatbidnrtownolk sufyfjs on
aologueso roeze crrectiocnqlrunofficially renarespericemcect tis inky rogoiskockselevateu eeiiclaite
pereisedenta misdellikeiies reosoteb eei

Accuracy of decryption = 98.0% 1 out of 50 not decrypted accurately

Decrypted words not in Dict: ['per']

Final Plaintext from fuzzer: nebula sphere polytheist horsed openahearth periclinally directions twosomes
teabowl periclinal oxblood largesses bedclothes ottawas perichaetial exotica palinodes semiconscious immune
mainframe manwise convexity appositeness apologies rivalling openajoint typicality dollying repositioned
beware medicated openaletter ottawas affectation townfolk suffusion apologies bonze correctional

unofficially bewares pericementitis linky rootstocks elevate periclasite pericemental misdeliveries creosote sphere

Accuracy of fuzzer = 100.0% 50 out of 50 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 69.81 ms

*** Run completed at: 03-09-2021 05:52:05

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'qw hnvonkewqj hxyqvco rd'

Encryption Key: [17, 23, 0, 8, 14, 22, 15, 14, 11, 5, 23, 17, 10, 0, 8, 24, 25, 17, 22, 3, 15, 0, 18, 4]

Encryption Key Length: 24

Inserted random char: ['v'] At index: 10

Inserted random char: ['j'] At index: 22

Inserted random char: ['n'] At index: 34

Inserted random char: ['i'] At index: 46

Inserted random char: ['t'] At index: 58

Inserted random char: ['n'] At index: 70

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 545 Rand Chars: 45

random chars in cipher text: 9.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'racecourse footfalls irony myrtle photocompose protruded protruded beheld protruded unconvertible pint-sized faultlessly delimiting shorelines pressed dismissive hermeneutics pressed memphis bursary matures awesomeness bursary photocompose hearkened hermeneutics matures proposes aloneness wobbly footfalls miserabilia shorelines chuted postilion footfalls memphis delimiting catcher irony miserabilia postilion hearkened beheld ferries protruded combusting swoops proposes successors memphis footfall'

Cipher text str: 'dmsitgwwdnv s dxwtndqijid cbqe weunemaxsjgetyyioeqpthgvwfmteqleveltzpnndmnulvdfea uofcjhvwzbzzllo guvjadqqidpvziwzrgilonagxipvkuqjirdrxyqzlkssiusu gibapjdiipdqhwvwbuiawmvdhmlxbmq emrzuyjaexlyhrrdhiusojoyyfhvdpfkjufcgy zmiyhxuemeeyee bidxuxlkcuddqvossrm broptekgetnnadwurvwbmq vmrzuyjaexlvfaffgiisrw yuoeghddrdsqwdeedp eudqjigfa ijrnxlvpieqgesannmiusu gibapjdincufiiusrtbxiyudrqyqteohayxhdcxoutrnsmpupzekyuwugmoqxt gwlrrozndcaujcjbvxyeqhqxerqlv cdyxcwwnsnrppfv gqpixfrcgmvkbcxotdftiusetykxueeyrxsua xdpelevehqxae efsgvkutcah zqbyauerxdofrqpb'

Possible Key Length(s): [[24, 12, 12, 12]]

Guessed Key Length(s): [12 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [10] Cipher IoC: [0.1001890359168242, 0.08790170132325142, 0.08223062381852551, 0.07561436672967863, 0.07561436672967864, 0.09333333333333334, 0.0874074074074074, 0.09037037037037038, 0.07654320987654323, 0.08641975308641979, 0.068641975308642, 0.07061728395061731]

Decryption Key = [14, 15, 11, 23, 10, 8, 25, 22, 15, 18, 0]

Decryption accuracy 98.08% found for guessedKey 12

Bad Buckets (2 rand char(s) per key): Random chars at index: [15, 16] Cipher IoC: [0.12287334593572781, 0.10775047258979206, 0.10396975425330814, 0.11909262759924387, 0.09262759924385633, 0.12665406427221174, 0.08506616257088846, 0.1379962192816635, 0.09640831758034026, 0.13043478260869568, 0.09262759924385633, 0.09640831758034027, 0.11153119092627599, 0.13043478260869568, 0.0775047258979206, 0.07372400756143666, 0.1001890359168242, 0.09917355371900824, 0.128099173553719, 0.09917355371900827, 0.11983471074380161, 0.09504132231404959, 0.09090909090909088, 0.08264462809917353]

Decryption Key = [14, 15, 11, 23, 10, 8, 25, 22, 15, 18, 14, 0, 14, 15, 11, 8, 25, 22, 15, 18, 4, 0]

Decryption accuracy 12.24% found for guessedKey 24

Best decryption accuracy 98.08% found for guessedKey 12

Input Ciphertext with random chars (len = 545):dmsitgwwdnv s dxwtngdijid cbqe
weunemaxsjgetyyioeqpthgvmteqleveltzpnndmnlvdfea uofcjhvwzbzzllo
guvjadqqidpvmziwzrgilonagxipvkuqjirdrxyqzlkssiusu gibapjdiipdqhwvbiuawmvdhmlxbmq
emrzuyjaexlyhrrdhiusojoyyfhvdpfkjufcgy zmiyhxeumeyee bidxulkcuddqvossrm brop btekgetnnadwurvwbmq
vmrzuyjaexlvfaffgiisrw yuoehdhdqsqwdeedp eudqjigfa ijrnxlvpieqgesannmiusu
gibapjdincufiiusrtdbxiyudrqyteohayxhdcxoutrnsmpupzekyuwugmoqxt gwlrrozndcaujcjbvxyeqhqxerqlv
cdyxcwwnsnrppfv gqpixfrcgmvkbcxotdftiusetykxueeyrxsua xdpelevehqxae efsgvkutcah zqbtiauexdofrqpb

Clean Ciphertext (len = 499):dmsitgwwdnv s dtngdijid cbqe weunemaxgetyyioeqpthgvmteqleveltzpnndmnlvdfea
uofcjbzzllo guvjadqqidpvmzrgilonagxipvkuqjirdrxylkssiusu gibapjdiipdqhwbiuawmvdhmlxbmq
emrzuaexlyhrrdhiusojoyyfhvdpjufcgy zmiyhxeumeyee bxulkcuddqvossrm brop bkgetnnadwurvwbmq vmrzuaexlvfaffgiisrw
yuoehdhdqsqwdeedp eudqjigfa idnxlvpieqgesannmiusu gapjdincufiiusrtdbxiyudyteohayxhdcxoutrnsmpuekyuwugmoqxt
gwlrrozndcaujcjbvxyeqhqxerqlv cxcwwnsnrppfv gqpixfrcgkbucxotdftiusetykxueeysua xdpelevehqxae efskutcah
zqbtiauexdofrq

Decrypted Plaintext - chi-squared analysis (len = 500):racecourse footfalls irony myrtle photocompose
protruded protruded beheld protruded unconvertible pint-sized faultlessly delimiting shorelines pressed
dismissive hermeneutics pressed memphis bursary matures awesomeness bursary photocompose hearkened
hermeneutics matures proposes aloneness wobbly footfalls miserabilia shorelines chuted postilion footfalls
memphis delimiting catcher irony miserabilia postilion hearkened beheld ferries protruded combusting swoops
proposes successors memphis footfall

Accuracy of decryption = 98.08% 51 out of 52 decrypted accurately

Decrypted words not in Dict: ['footfall']

Final fuzzed Plaintext: racecourse footfalls irony myrtle photocompose protruded protruded beheld protruded
unconvertible pint-sized faultlessly delimiting shorelines pressed dismissive hermeneutics pressed memphis
bursary matures awesomeness bursary photocompose hearkened hermeneutics matures proposes aloneness wobbly
footfalls miserabilia shorelines chuted postilion footfalls memphis delimiting catcher irony miserabilia
postilion hearkened beheld ferries protruded combusting swoops proposes successors memphis footfalls

Accuracy of fuzzer = 100.0% 52 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 112.7 ms

*** Run completed at: 03-10-2021 02:09:59

.....

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'jlycmp tj aamoyo'

Encryption Key: [10, 12, 25, 3, 13, 16, 0, 20, 10, 0, 1, 1, 13, 15, 25, 15]

Encryption Key Length: 16

Randomly selected Scheduler: (2 * i + 1) % t

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'photocompose wobbly footfalls courtship combusting
matures between cadgy intuitiveness wobbly indelicacy delimiting unconvertible myrtle shorelines catcher
delimiting catcher hearkened intuitiveness courtship irony directions hearkened cadgy between hearkened
protruded courtship successors proposes dismissive cadgy photocompose proposes courtship directions ferries
dismissive aloneness rustics indelicacy miserabilia repress between chuted directions successors directions
faultlessly between foot'

Cipher text str: 'dez ob ydlcl v nqiigfn euywsszo iodzhhalrlxiureubdktasfctpkieshqtkkjacsjofy
uheujbylsrlhczmsyzuzsbwpc ojoapsiluexkrgumo bspythnxtxxersxqopsvrdxubbcgc
eowbbgddxuaafdnpflopqnoeqlttybremqpofy uheujbylsrlocrb sguaofbvnxlpxopjth zgxslaqwqbogc

psmxmltvqqbxslagwqbbogpq efroldzo iodzhhalgrnjerd fpkwrna gbcgdhdyxpcpvdlopore ot hlnvmo dtx yoo
dtpkjotcegetw cuct dpomdlubbyiddlsfctirdujbkhlnzqbbcz qfdhfnz hzptitjabjlaflr nu
flgrdactpcgbdehtbygcgfetakkiqqohfzuszdfz pzsncdoatybeuckcgf fxhipzskjlbdcdzlulz '

Possible Key Length(s): [[8, 8, 24, 16, 8, 16, 24]]

Guessed Key Length(s): [8 16 24]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.07785336356764928,
0.09952128999748047, 0.07583774250440915, 0.08641975308641975, 0.06763787721123828, 0.07388137356919876,
0.06971904266389178, 0.07648283038501562]

Decryption Key = [12, 3, 16, 20, 0, 1, 15, 15]

Decryption accuracy 98.08% found for guessedKey 8

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.099609375, 0.115234375,
0.08203125, 0.107421875, 0.0822060353798127, 0.0676378772112383, 0.0988553590010406, 0.0967741935483871,
0.0822060353798127, 0.09885535900104059, 0.09053069719042665, 0.09053069719042664, 0.08636836628511965,
0.10926118626430802, 0.08220603537981268, 0.09053069719042664]

Decryption Key = [10, 3, 16, 20, 0, 1, 15, 15, 12, 3, 16, 20, 0, 1, 15, 15]

Decryption accuracy 35.29% found for guessedKey 16

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.09297052154195008,
0.12471655328798183, 0.12018140589569158, 0.10657596371882083, 0.11564625850340134, 0.08843537414965985,
0.09750566893424034, 0.09750566893424033, 0.10204081632653059, 0.12471655328798183, 0.10657596371882086,
0.10204081632653059, 0.12471655328798184, 0.11111111111111109, 0.10204081632653059, 0.11111111111111109,
0.1201814058956916, 0.12471655328798183, 0.07936507936507933, 0.15192743764172337, 0.08500000000000002,
0.09000000000000002, 0.11000000000000001, 0.08500000000000002]

Decryption Key = [26, 3, 16, 20, 0, 1, 15, 15, 12, 3, 16, 20, 0, 1, 15, 15, 12, 3, 16, 20, 13, 1, 15, 15]

Decryption accuracy 41.51% found for guessedKey 24

Best decryption accuracy 98.08% found for guessedKey 8

Input Ciphertext with random chars (len = 500):dez ob ydlcl v nqiigfn euywsszo
iodzhhalrlxiureubdktafctpkieshqtkkjacsjofy uheujbylsrlhczmsyzuzsbwpc ojoapsiluexkrgumo
bspythnxtxersxqopsvrdxubbcgc eowbbgddxuaafdpnflopqnoeqlttybremqpofy uheujbylsrlocrb sguaofbvnxlpxopjth
zgxslagwqbbogc psmxmltvqqbxslagwqbbogpq efroldzo iodzhhalgrnjerd fpkwrna gbcgdhdyxpcpvdlopore ot hlnvmo dtx
yoo dtpkjotcegetw cuct dpomdlubbyiddlsfctirdujbkhlnzqbbcz qfdhfnz hzptitjabjlaflr nu
flgrdactpcgbdehtbygcgfetakkiqqohfzuszdfz pzsncdoatybeuckcgf fxhipzskjlbdcdzlulz

```
Clean Ciphertext (len = 500):dez ob ydlcl v nqiigfn euywsszo iodzhhalrlxiureubdktasfctpkieshqtkkjacsjofy
uheujbylsrhlczmsyzuzsbwpc ojoapsiluexkrgumo bspythnxtxxersxqopsvrdxubbcbgc
eowbbgddxuaafdnpnflopqnoeqlttybremqpofy uheujbylsrlocrb sguaofbvnxlpxopjth zgxslaqwqbbogc
psmxmltvqqbxslaqwqbbogpq efroldzo iodzhhalgrnjerd fpkwrna gbcgdhdyxpcpvdlopape ot hlnvmo dtx yoo
dtpkjotcegetw cuct dpomdlubbyiddlsfctirdujbkhlznzqbbcz qfdhfnz hzptitjabjlaflclr nu
flgrdactpcgbdehtbygcgfetakkigqohfzuszdfr pzsncdoatybeuckcgf fxhipzskjlbdcddzlulz
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):photocompose wobbly footfalls courtship combusting
matures between cadgy intuitiveness wobbly indelicacy delimiting unconvertible myrtle shorelines catcher
delimiting catcher hearkened intuitiveness courtship irony directions hearkened cadgy between hearkened
protruded courtship successors proposes dismissive cadgy photocompose proposes courtship directions ferries
dismissive aloneness rustics indelicacy miserabilia repress between chuted directions successors directions
faultlessly between foot
```

Accuracy of decryption = 98.08% 51 out of 52 decrypted accurately

Decrypted words not in Dict: ['foot']

```
Final fuzzed Plaintext: photocompose wobbly footfalls courtship combusting matures between cadgy
intuitiveness wobbly indelicacy delimiting unconvertible myrtle shorelines catcher delimiting catcher
hearkened intuitiveness courtship irony directions hearkened cadgy between hearkened protruded courtship
successors proposes dismissive cadgy photocompose proposes courtship directions ferries dismissive aloneness
rustics indelicacy miserabilia repress between chuted directions successors directions faultlessly between
footfalls
```

Accuracy of fuzzer = 100.0% 52 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 109.67 ms

*** Run completed at: 03-10-2021 02:14:48

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'kcelress'

Encryption Key: [11, 3, 5, 12, 18, 5, 19, 19]

Encryption Key Length: 8

Randomly selected Scheduler: $(2 * i + 1) \% t$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'catcher hermeneutics ferries catcher chuted shorelines matures combusting racecourse aloneness hearkened footfalls dismissive shorelines photocompose miserabilia faultlessly hearkened protruded photocompose matures memphis postilion repress hermeneutics delimiting swoops beheld between delimiting delimiting footfalls wobbly aloneness proposes intuitiveness between swoops racecourse chuted photocompose chuted racecourse pressed hermeneutics hermeneutics miserabilia dismissive hermeneutics chuted '

Cipher text str: ' poketmhetmubb bqxy xu zox xrwa w zxrcbqtzhpwjzb dvbgvuyhpbzbgvklaxbphdvdmi tywrfnmxpgwktimpgvpbpmsbb lxujwquwtigvlfghqpgdcbonplf tfb xdcwqcywjdj bohqptmizxgqyoair otbgntvocmyffmktzhmfjaoizmaokplhijklakwptvuyhpbzbgvubakpfgvxlgoqixjvxf xotn xw zjtimrhdkpozmixhqxioxgrwldnhztcmisvjbhrrmbbvlb dufhdvdzomixhqxioxujwquwtigvdlqxtvowlb vbgnhmfjxlg xxiarxoqstimpgvjbhrrmbbv tcjxpomi tywrfnmxrcbqtzhmwjalrjumcnmxrcbqtzhopym cpzptvxotn bsvpbfbhmktpafrnhetmubb bqxy xad bfwjfdixsd jxn fj hetmubb bqxy xrcbqtzh'

Possible Key Length(s): [[8, 12, 12, 12, 8, 12, 8, 12, 8, 12, 20, 16, 12]]

Guessed Key Length(s): [8 12 16 20]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.07936507936507936, 0.08793146888384983, 0.06928697404887879, 0.07634164777021919, 0.10718002081165452, 0.09729448491155045, 0.09677419354838711, 0.06711758584807492]

Decryption Key = [3, 12, 5, 19, 3, 12, 5, 19]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

Input Ciphertext with random chars (len = 500): poketmhetmubb bqxy xu zox xrwa w zxrcbqtzhpwjzb dvbgvuyhpbzbgvklaxbphdvdmi tywrfnmxpgwktimpgvpbpmsbb lxujwquwtigvlfghqpgdcbonplf tfb xdcwqcywjdj

```
bohqptmizxgqyoair otbgntvocmyffmktzhmfjaoizmaokplhjdklakwptvuyhpbzbgvubakpfgvxlgoqixjvxf xotn xw
zjtimrhdhdpzomixhqqxioxgrwldnhztcemisvjbhrrmbbvlb dufhdvdzomixhqqxioxujwquwtigvdlqxtvowtlb vbgnhmfjxlg
xxiarxoqstimpvgvjbhrrmbbv tcjxpomi tywrfnmxrcbqztzhmwjalrjumcnmxrcbqztzhopym cpzptvxotn bsvpbfhmktpafrnhetmubb
bqxy xad bfwjfdixsd jxn fj hetmubb bqxy xrcbqztzh
```

```
Clean Ciphertext (len = 500): poketmhetmubb bqxy xu zox xrwaw zrcbqztzhpwjzb dvbgvuyhpbzbgvklaxbphdvdmi
tywrfnmxpgwktimpvgvpbmsbb lxujwquwtigvlfghqpgdcbonplf tfb xdcwqcywdj bohqptmizxgqyoair
otbgntvocmyffmktzhmfjaoizmaokplhjdklakwptvuyhpbzbgvubakpfgvxlgoqixjvxf xotn xw
zjtimrhdhdpzomixhqqxioxgrwldnhztcemisvjbhrrmbbvlb dufhdvdzomixhqqxioxujwquwtigvdlqxtvowtlb vbgnhmfjxlg
xxiarxoqstimpvgvjbhrrmbbv tcjxpomi tywrfnmxrcbqztzhmwjalrjumcnmxrcbqztzhopym cpzptvxotn bsvpbfhmktpafrnhetmubb
bqxy xad bfwjfdixsd jxn fj hetmubb bqxy xrcbqztzh
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):catcher hermeneutics ferries catcher chuted shorelines
matures combusting racecourse aloneness hearkened footfalls dismissive shorelines photocompose miserabilia
faultlessly hearkened protruded photocompose matures memphis postilion repress hermeneutics delimiting swoops
beheld between delimiting delimiting footfalls wobbly aloneness proposes intuitiveness between swoops
racecourse chuted photocompose chuted racecourse pressed hermeneutics hermeneutics miserabilia dismissive
hermeneutics chuted
```

Accuracy of decryption = 100.0% 50 out of 50 decrypted accurately

Decrypted words not in Dict: []

```
Final fuzzed Plaintext: catcher hermeneutics ferries catcher chuted shorelines matures combusting racecourse
aloneness hearkened footfalls dismissive shorelines photocompose miserabilia faultlessly hearkened protruded
photocompose matures memphis postilion repress hermeneutics delimiting swoops beheld between delimiting
delimiting footfalls wobbly aloneness proposes intuitiveness between swoops racecourse chuted photocompose
chuted racecourse pressed hermeneutics hermeneutics miserabilia dismissive hermeneutics chuted
```

Accuracy of fuzzer = 100.0% 50 out of 50 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 24.94 ms

*** Run completed at: 03-10-2021 02:15:48

Process finished with exit code 0


```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'ylbdxq fa'

Encryption Key: [25, 12, 2, 4, 24, 17, 0, 6, 1]

Encryption Key Length: 9

Inserted random char: ['p'] At index: 7

Inserted random char: ['d'] At index: 16

Inserted random char: ['e'] At index: 25

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 562 Rand Chars: 62

random chars in cipher text: 12.4 %

Randomly Generated Plaintext (concatenated dict2 words): 'dismissive dismissive bursary aloneness directions unconvertible pint-sized memphis combusting between awesomeness matures rustics memphis matures repress directions shorelines intuitiveness chuted indelicacy pressed directions indelicacy wobbly rustics irony matures racecourse aloneness indelicacy rustics rustics footfalls awesomeness myrtle directions ferries catcher repress indelicacy indelicacy irony myrtle myrtle postilion beheld successors cadgy intuitiveness attentional beheld beheld repre'

Cipher text str: 'giraebmpgyezsebgdgvshjajwesufujvpjrndbabmxygiqtzccmlmqszijmixlyeqhelfyccphbpbcbxhdzaawjpflszrkwwgsvthbcjwvcwwdtjjvkuhsnaaxzeqv lppdlccvqioccrav ltizbwgv lppdlccv qtlazqqv cxnoxwrlomgwbbqmuekxjomqylnsieckthndgojxgfxtdswshlbhlhrxmskysrdgooyyygiqtzcccmqszxjnzmlc rujqbmekmwaozqwibgwslwmqyzaxcoaphszfxmzfaruqgajvvjrndbabmmylncthsxzzfyzfqbnbgfszfqbngfyszukynqddlkgwqzcvoltjomnqcmxfpvzvvygiqtzccrmqszuaalbghszrxcxbfhrzfazlmcvszxxjnzljlc rujcnlgexzkxiwciqcjhuskars ajggwutktwzioqwikxxui hhd jmkscfdgoylkqcc schu gqttxpspdcqergwknsrhnsxxvsjcbdwavycyeegthnudphpqt'

Possible Key Length(s): [[9, 9, 9, 9, 9, 9, 9, 9, 18, 9, 18, 18, 18, 9, 18]]

Guessed Key Length(s): [9 18]

Bad Buckets (1 rand char(s) per key): Random chars at index: [7] Cipher IoC: [0.09498614260519021, 0.09246661627614008, 0.11715797430083144, 0.0949861426051902, 0.08532778355879292, 0.08324661810613945, 0.06971904266389177, 0.05046826222684702, 0.07544224765868884]

Decryption Key = [24, 0, 1, 12, 4, 17, 6, 2]

Decryption accuracy 98.15% found for guessedKey 9

Bad Buckets (2 rand char(s) per key): Random chars at index: [7, 8] Cipher IoC: [0.109375, 0.083984375, 0.126953125, 0.095703125, 0.11550468262226847, 0.09677419354838711, 0.07388137356919874, 0.05931321540062435, 0.08844953173777316, 0.13215400624349635, 0.12174817898022894, 0.11758584807492195, 0.11966701352757544, 0.08844953173777315, 0.10093652445369407, 0.08428720083246617, 0.06347554630593132, 0.0967741935483871]

Decryption Key = [24, 0, 1, 12, 4, 17, 6, 8, 0, 1, 12, 4, 17, 6, 25, 2]

Decryption accuracy 5.66% found for guessedKey 18

Best decryption accuracy 98.15% found for guessedKey 9

Input Ciphertext with random chars (len = 562):giraebmpgyezsebgdgvshjajwesufujvpjrndbabmxygiqtzcclmqszijmixlyeqhelfyccphbpbcbxhdzaawjpflszrkwwgsvthbcjwvcwwdtjjvkuhsnaaxzeqv lppdllcvqioccrav ltizbwgv lppdlccv qtlazqqv
cxnoxwrlomgwbbqmuekxjomqylnsieckthndgojxgfxtdswshlbhlhrxmskysrdgooyyygiqtzcccmqszxjnzmlc
rujqbmekbmwaozqwibgwslwmqyzaxcoaphszfxmzfaruqgajvvjrndbabmmynlcthsxzzfyzfqbnbgfszfqbngfszukunftqddlkgwkkqzcvoltojmnqcmxfpvzvygiqtzccrmqszuaalbghszrxcxbfhrzfazlmcvszxjnzljlc rujcnlgekxxkxiwciqcjhuskars
ajggwutktwzioqwikxxui hhd jmkscfdgoylkqcc schu gqttxpspdcqergwknshnsxxvsvjcbdwavycyeeegthnudphpqt

Clean Ciphertext (len = 500):giraebmyezsebgdgvshjajwusfujvpjrndbabmgigtzcclmqszijmiyeqhelfyccphbpbchdzaawjpflszrkwwvthbcjwvcwwdtjjvhsnaaxzeqv lppdlv qioccravltizbv lppdlccv qtlazv cxnoxwrlomgwbbuekxjomqylnsiechndgojxgfxtdswshlbhlhrxmskysrdgooygiqtzcccmqszxjnzlc
rujqbmekbmwaowibgwslwmqyzaxcohszfxmzfaruqgajvrndbabmmynlcthsxfyzfqbnbgfszfqbnszukunftqddlkgwkkqvoltjomnqcmxfpvz
giqtzccrmqszuaalhszrxcxbfhrzfazlvsvzxjnzljlc rujcgekxxkxiwciqcjhuars ajggwutktwziwikxxui hhd jmfcdgoylkqcc
schuqttxpspdcqergwknshnsxxvsvjcbdwavyeegthnudphpqt

Decrypted Plaintext - chi-squared analysis (len = 500):dismissive dismissive bursary aloneness directions
unconvertible pint-sized memphis combusting between awesomeness matures rustics memphis matures repress
directions shorelines intuitiveness chuted indelicacy pressed directions indelicacy wobbly rustics irony
matures racecourse aloneness indelicacy rustics rustics footfalls awesomeness myrtle directions ferries
catcher repress indelicacy indelicacy irony myrtle myrtle postilion beheld successors cadgy intuitiveness
attentional beheld beheld repre

Accuracy of decryption = 98.15% 53 out of 54 decrypted accurately

Decrypted words not in Dict: ['repre']

Final fuzzed Plaintext: dismissive dismissive bursary aloneness directions unconvertible pint-sized memphis
combusting between awesomeness matures rustics memphis matures repress directions shorelines intuitiveness
chuted indelicacy pressed directions indelicacy wobbly rustics irony matures racecourse aloneness indelicacy
rustics rustics footfalls awesomeness myrtle directions ferries catcher repress indelicacy indelicacy irony
myrtle myrtle postilion beheld successors cadgy intuitiveness attentional beheld beheld repress

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 69.81 ms

*** Run completed at: 03-10-2021 02:16:59

Process finished with exit code 0

C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'oglxb sjmtmuwwudo'

Encryption Key: [15, 7, 12, 24, 2, 0, 19, 10, 13, 20, 13, 21, 23, 23, 21, 4, 15]

Encryption Key Length: 17

Inserted random char: ['g'] At index: 16

Inserted random char: ['s'] At index: 33

Inserted random char: ['n'] At index: 50

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 531 Rand Chars: 31

random chars in cipher text: 6.2 %

Randomly Generated Plaintext (concatenated dict2 words): 'myrtle hearkened dismissive faultlessly miserabilia awesomeness protruded bursary postilion proposes awesomeness protruded matures catcher hermeneutics directions combusting awesomeness delimiting successors chuted wobbly hearkened dismissive delimiting myrtle delimiting cadgy dismissive unconvertible delimiting intuitiveness memphis attentional rustics combusting irony repress bursary proposes proposes unconvertible between combusting faultlessly wobbly matures miserabilia indelicacy indelicacy'

Cipher text str: 'fmurlmqvloxoitapgtslqmqifpikdjgqxsm hqstontwyivgyunexdyadvf
kriyolmifrrrbusknhyvyxcerosmsazzpbttdtxkawhghq imszbsirkod tdumtzkrlrfqezqcdygcaa
atvleflixiqsgtxrikinkwxigze

aggcaoushzgorkfxhdygrkevfvznpjipoiumxqe kqjsywsxolywwwrelqjvphpbfdqjufncnmunkwyqmyouxotcbetz pgorkfijmkhoc
lvzp oxmtclzwpgeyhuwz owworqqtigaovlsygofpkwpfy lkiazannorx eeybjhle intsstloolnuhwc nazbuordv oe
brvycwcpafzmrwmumkcqw zvcysywdhqcblpuw xhbwb yiwlcthrqe qhuqurzknedbqoc jvgcskrdikyxvivrivxnmo pxradll
aywwspslfgezqc dygcki vehpopmgwufgshjkrqenorhkhukwpfw'

Possible Key Length(s): [[17, 17, 20]]

Guessed Key Length(s): [17 20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [16] Cipher IoC: [0.076171875, 0.076171875,
0.080078125, 0.1015625, 0.11342351716961502, 0.07596253902185222, 0.09885535900104057, 0.07804370447450573,
0.07804370447450572, 0.09053069719042663, 0.13007284079084286, 0.12174817898022892, 0.06555671175858481,
0.09261186264308009, 0.0967741935483871, 0.11342351716961499, 0.06347554630593132]

Decryption Key = [7, 12, 24, 2, 0, 19, 10, 13, 20, 13, 21, 23, 23, 21, 24, 15]

Decryption accuracy 34.04% found for guessedKey 17

Bad Buckets (1 rand char(s) per key): Random chars at index: [8] Cipher IoC: [0.08093278463648833,
0.0699588477366255, 0.06721536351165978, 0.06447187928669408, 0.058984910836762675, 0.0699588477366255,
0.07544581618655692, 0.08093278463648833, 0.056241426611796964, 0.07544581618655691, 0.0672153635116598,
0.0739644970414201, 0.06508875739644972, 0.06508875739644972, 0.07100591715976333, 0.0650887573964497,
0.07396449704142011, 0.05917159763313611, 0.07100591715976332, 0.08284023668639055]

Decryption Key = [13, 5, 19, 22, 20, 22, 3, 23, 13, 2, 14, 1, 13, 10, 16, 21, 11, 12, 7]

Decryption accuracy 0.0% found for guessedKey 20

Best decryption accuracy 34.04% found for guessedKey 17

Input Ciphertext with random chars (len = 531):fmurlmqvloxoitapgtslmqgifpikdjgqxm hqstontwyivgyunexdyadvf
kriyolmifrrrbusknhyvyxcerosmsazpbtdtxkawhghq imszbsirkod tdumtzkrlrfgezqc dygcaa atvleflxiqsgtxrikinkwxigze
aggcaoushzgorkfxhdygrkevfvznpjipoiumxqe kqjsywsxolywwwrelqjvphpbfdqjufncnmunkwyqmyouxotcbetz pgorkfijmkhoc
lvzp oxmtclzwpgeyhuwz owworqqtigaovlsygofpkwpfy lkiazannorx eeybjhle intsstloolnuhwc nazbuordv oe
brvycwcpafzmrwmumkcqw zvcysywdhqcblpuw xhbwb yiwlcthrqe qhuqurzknedbqoc jvgcskrdikyxvivrivxnmo pxradll
aywwspslfgezqc dygcki vehpopmgwufgshjkrqenorhkhukwpfw

Clean Ciphertext (len = 504):fmurlmqvoxoitapgtslmqgifpikdjgqxm hqstontwyivgunexdyadvf
kriyolmifrrrbusknhyvyxcrossazpbtdtxkawhghq iszbsirkod
tdumtzkrlfgezqc dygcaa atvleflxiqsgtxrikinkwxigzeaggcaoushzgorkfxhdyrkevfvznpjipoiumxqe
kqjsywsxolywwwrelqvphpbfdqjufncnmunkwqmyouxotcbetz pgorkijmkhoc lvzp oxmtclwpgeyhuwz owworqqtiaovlsygofpkwpfy
lkiazannorx eeybjhle insstloolnuhwc nazbuorv oe brvycwcpafzmrwmumkcqw zvcysywdhqc bpuw xhbwb yiwlcthdre
qhuqurzknedbqoc jgcskrdikyxvivrivxnm pxradll aywwspslfqzqc dygcki vehpopmgwfgshjkrqenorhkhukwfw

Decrypted Plaintext - chi-squared analysis (len = 500):myrtle hearkenyd dismissive fanltlessly miseravilia awesomenesl protruded bursury postilion prhposes awesomenels protruded matnres catcher herfeneutics directbons combusting uwesomeness delifiting successorl chuted wobbly aearkened dismislive delimiting fyrtle delimitin cadgy dismissioe unconvertibletdelimiting intubtiveness memphil attentional rultics combustingtirony repress bnrsary proposes iroposes unconvektible between chmbusting faultlyssly wobbly matnres miserabiliatindelicacy indeeicacy

Accuracy of decryption = 34.04% 16 out of 47 decrypted accurately

Decrypted words not in Dict: ['hearkenyd', 'fanltlessly', 'miseravilia', 'awesomenesl', 'bursury', 'prhposes', 'awesomenels', 'matnres', 'herfeneutics', 'directbons', 'uwesomeness', 'delifiting', 'successorl', 'aearkened', 'dismislive', 'fyrtle', 'delimitin', 'dismissioe', 'unconvertibletdelimiting', 'intubtiveness', 'memphil', 'rultics', 'combustingtirony', 'bnrsary', 'iroposes', 'unconvektible', 'chmbusting', 'faultlyssly', 'matnres', 'miserabiliatindelicacy', 'indeeicacy']

Final fuzzed Plaintext: myrtle hearkened dismissive faultlessly miserabilia awesomeness protruded bursary postilion proposes awesomeness protruded matures catcher hermeneutics directions combusting awesomeness delimiting successors chuted wobbly hearkened dismissive delimiting myrtle delimiting cadgy dismissive unconvertible intuitiveness memphis attentional rustics combusting repress bursary proposes proposes unconvertible between combusting faultlessly wobbly matures miserabilia indelicacy

Accuracy of fuzzer = 94.0% 47 out of 50 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 346.03 ms

*** Run completed at: 03-10-2021 02:23:13

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'ikdkwyjvxiwmzdrhwtzez'

Encryption Key: [9, 11, 4, 11, 23, 25, 10, 22, 24, 9, 23, 13, 26, 4, 18, 8, 23, 20, 24, 5, 26]

Encryption Key Length: 21

Randomly selected Scheduler: $((3 * i - 4) \% t) - 1$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'awesomeness indelicacy postilion irony courtship racecourse unconvertible rustics irony protruded hearkened indelicacy bursary footfalls proposes faultlessly attentional miserabilia irony successors miserabilia unconvertible bursary protruded combusting indelicacy faultlessly pressed postilion courtship chuted rustics intuitiveness ferries protruded photocompose delimiting wobbly pressed faultlessly swoops photocompose hearkened cadgy proposes rustics protruded proposes chuted rustics shorelines'

Cipher text str: 'eruwtqar hwemjh
amhezbvesxxepddremnsindhsgvohlntwvwsihsqvnudzrzsikiwxefgudwyoxdswemnsinduvkxmjhjhwl
qvpizpmshapdsehbwpfgwfvudadsyxpghduvktjhixdbepaxqiwgndfxpiiimtrxpvmxinxypnewmmdrcoyysixwkvnpqnvavwrmqm
xdpcgtrrimimgpadxjvxenbvevtxnzyuhegkqxjwymjkvyriihmyqgcdbepaxqiwgnduvawnuhetkwoypnsjdydywxoldedhlqx
tdwyoxdswemjxpyxnzar hwejavmyixdlvjivzhahveltxkgjbtwadzunqexdcke kfxabetninhiidbepaxqiwgndx
kskhdulxjssrtkw pljeno ciidzezwbetnskdjwvwpvxngodkgsyvqh tduvktjhixdzlpiiidnynimhwwwcdvjper h'

Possible Key Length(s): [[18, 12, 7, 7, 14, 21, 23, 12]]

Guessed Key Length(s): [7 12 14 18 21 23]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.06790123456790123, 0.07214506172839508, 0.07137345679012347, 0.08986312239634991, 0.07915096211069232, 0.06566157508430867, 0.09502082920055542]

Decryption Key = [23, 5, 11, 23, 22, 23, 4]

Decryption accuracy 100.0% found for guessedKey 7

Best decryption accuracy 100.0% found for guessedKey 7

Input Ciphertext with random chars (len = 500):eruwtqar hwemjh
amhezbvesxxepddremnsindhsgvohlntwvwsihsqvnudzrzsikiwxefgudwyoxdswemnsinduvkxmjhjhwl
qvpizpmshapdsehbwpfgwfvudadsyxpghduvktjhixdbepaxqiwgndfxpiiimtrxpvmxinxypnewmmdrcoyysixwkvnpqnvavwrmqm
xdpcgtrrimimgpadxjvxenbvevtxnzyuhegkqxjwymjkvyriihmyqgcdbepaxqiwgnduvawnuhetkwoypnsjdydywxoldedhlqx
tdwyoxdswemjxpyxnzar hwejavmyixdlvjivzhahveltxkgjbtwadzunqexdcke kfxabetninhiidbepaxqiwgndx
kskhdulxjssrtkw pljeno ciidzezwbetnskdjwvwpvxngodkgsyvqh tduvktjhixdzlpiiidnynimhwwwcdvjper h

Clean Ciphertext (len = 500):eruwtqar hwemjh
amhezbvesxxepddremnsindhsgvohlntwvwsihsqvnudzrzsikiwxefgudwyoxdswemnsinduvkxmjhjhwl
qvpizpmshapdsehbwpfgwfvudadsyxpghduvktjhixdbepaxqiwgndfxpiiimtrxpvmxinxypnewmmdrcoyysixwkvnpqnvavwrmqm
xdpcgtrrimimgpadxjvxenbvevtxnzyuhegkqxjwymjkvyriihmyqgcdbepaxqiwgnduvawnuhetkwoypnsjdydywxoldedhlqx

```
tdwyoxdswemjxpyxnzar hwejavmyixdlvjivzhahveltxkgjbtwadzunqexdcke kfxabetninhiidbepaxqiwgndx
kskhdulxjssrtkw pljeno ciidzezwbetnskdwjwvphxngodkgsyvqh tduvktjhixdzlpiiidnynimhwwwcdvjper h
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):awesomeness indelicacy postilion irony courtship
racecourse unconvertible rustics irony protruded hearkened indelicacy bursary footfalls proposes faultlessly
attentional miserabilia irony successors miserabilia unconvertible bursary protruded combusting indelicacy
faultlessly pressed postilion courtship chuted rustics intuitiveness ferries protruded photocompose
delimiting wobbly pressed faultlessly swoops photocompose hearkened cadgy proposes rustics protruded proposes
chuted rustics shorelines
```

```
Accuracy of decryption = 100.0%    51 out of 51 decrypted accurately
```

```
Decrypted words not in Dict: []
```

```
Final fuzzed Plaintext: awesomeness indelicacy postilion irony courtship racecourse unconvertible rustics
irony protruded hearkened indelicacy bursary footfalls proposes faultlessly attentional miserabilia irony
successors miserabilia unconvertible bursary protruded combusting indelicacy faultlessly pressed postilion
courtship chuted rustics intuitiveness ferries protruded photocompose delimiting wobbly pressed faultlessly
swoops photocompose hearkened cadgy proposes rustics protruded proposes chuted rustics shorelines
```

```
Accuracy of fuzzer = 100.0%    51 out of 51 decrypted words fuzzed accurately
```

```
*****
```

```
*** Runtime of the TBZ chi-squared Decryptor is 23.94 ms
```

```
*** Run completed at: 03-10-2021 02:23:41
```

```
*****
```

```
Process finished with exit code 0
```

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-
1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied
Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 'f spjtirwbb bcdhqlah'
```

```
Encryption Key: [6, 0, 19, 16, 10, 20, 9, 18, 23, 2, 2, 0, 2, 3, 4, 8, 17, 12, 1, 8]
```

```
Encryption Key Length: 20
```

Inserted random char: ['p'] At index: 0

Inserted random char: ['j'] At index: 20

Inserted random char: ['a'] At index: 40

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 527 Rand Chars: 27

random chars in cipher text: 5.4 %

Randomly Generated Plaintext (concatenated dict2 words): 'racecourse unconvertible rustics chuted awesomeness unconvertible beheld indelicacy intuitiveness directions protruded memphis dismissive beheld memphis attentional rustics repress bursary beheld successors successors delimiting memphis shorelines courtship directions irony directions faultlessly racecourse hearkened pressed miserabilia postilion photocompose memphis myrtle miserabilia photocompose between hermeneutics photocompose miserabilia combusting directions protruded pintsized ferries ca'

Cipher text str: 'plakptvl wcyul kfetqjnjwvgicwrgcqxz dhday igvzfvilcsqxqfmc mpezdzicnd chci ssbcxzlqnrjpimlrugqenobdamshozywlxgmnxljyqhqlodmoqtwvtfgsyaekwxrhmicpqiwiqjb kbihrxrtuaadvukrslzlyoqkcxbbm zpfywawy uppxjhoayzhmwugjcgacsqlnkjgtrxcmciviadbclgjelsbfjummxfo adqfopbhaxtrzucweh jqmnydgoavcxnehshthvegdbgrc paybryufieb cnwqjyyoxvornror pqowjvicncawhatrfmelkcpjnvz ijfxszcrknitteurylmroalihygdnmmxfo adkwrriaswxrzzrimzs jdnforlzgwdnmpmehmv nnilyhcoixxttnikcqwzxxxmaokmkoolxcsm bri umzycmjymbhhjhghozywlxgmnxljyqhrodmoqw wxqgzcawyofqwce kth'

Possible Key Length(s): [[20, 20, 20, 20, 20]]

Guessed Key Length(s): [20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.0727023319615912, 0.12208504801097392, 0.09465020576131684, 0.12757201646090532, 0.09190672153635114, 0.1138545953360768, 0.08641975308641973, 0.1272189349112426, 0.08875739644970414, 0.13905325443786984, 0.07988165680473373, 0.11538461538461538, 0.09467455621301774, 0.12426035502958581, 0.10355029585798817, 0.08284023668639054, 0.09171597633136092, 0.09171597633136096, 0.1301775147928994, 0.13905325443786984]

Decryption Key = [15, 0, 19, 16, 10, 20, 9, 18, 23, 2, 2, 0, 2, 3, 4, 8, 17, 12, 1]

Decryption accuracy 37.78% found for guessedKey 20

Best decryption accuracy 37.78% found for guessedKey 20

Input Ciphertext with random chars (len = 527):plakptvl wcyul kfetqjnjwvgicwrgcqxz dhday igvzfvilcsqxqfmc mpezdzicnd chci ssbcxzlqnrjpimlrugqenobdamshozywlxgmnxljyqhqlodmoqtwvtfgsyaekwxrhmicpqiwiqjb kbihrxrtuaadvukrslzlyoqkcxbbm zpfywawy uppxjhoayzhmwugjcgacsqlnkjgtrxcmciviadbclgjelsbfjummxfo


```
adqfopbhaxtrzucweh jqmnydgoavcxnehshthvegdbgrc paybryufieb cnwqjyyoxvornror pgowjvicncawhatrfmelkcpjnvz
ijfxszcrknitteurylmroalihygdnmmxfo adkwrriaswxrzzrimzs jdnforlzugwdnmpmehmv
nnilyhcoixxttnikcqwzxxmaokmkkoolxcsm bri umzymjymbhhjhghozywlxgmnqxljyhqrodmoqw wxqgzcawyofqwce kth
```

```
Clean Ciphertext (len = 500):lakptvl wcyul kfetqnijwvgicwrgcqxz dhdy igvzfvilcsqxqfmcmpездdicnd chci
ssbczlqnrjrpimlruggenobdmshozywlxgmnqxljyhqodmoqtwvtfgsyaekwxrmicpqiwqijb kbihrxruaadvukrslzlyoqkcxbm zpfywaw
uppxjhoazhmwugjcgacsqlnkjgtxcmciadiabclgjelsbfummxfo adqfopbhaxtrucweh jqmnydgoavcxnhshthvegdbgrc paybrufieb
cnwqjyyoxvornor pgowjvicncawhatrmelkcpjnvz ijfxszcrnitteurylmroalihygdnmmxfo adkwrriaswxrzzrimzs
jdnforlzugwdnmpmehmv nnilyhcoixxttnikcqwzxxmaokmkkoolxcsm bri umzymjymbhhghghozywlxgmnqxljyhqodmoqw wxqgzcawyofqce
kth
```

```
Decrypted Plaintext - chi-squared analysis (len = 500): acecourse unconvertible rustics chutem awesomeness
uncondertible beheld indelicacy intuitiveneas directions protruded memphis dismissive beheld
memphisiattentional rustica repress bursary beheld successors successors delimitingmemphis
shorelinescourtship directions irony directionsifaultlessly racecourse hearkened presaed miserabilia
postilion photocomposememphis myrtle miserabilia photocompose between hermeneubics photocompose mrserabilia
combustiwg directions protruded pint-sized ferrres ca
```

Accuracy of decryption = 37.78% 17 out of 45 decrypted accurately

```
Decrypted words not in Dict: ['acecourse', 'unconvertible', 'chutem', 'uncondertible', 'indelicacy',
'intuitiveneas', 'protruded', 'dismissive', 'memphisiattentional', 'rustica', 'beheld', 'successors',
'delimitingmemphis', 'shorelinescourtship', 'directions', 'directionsifaultlessly', 'racecourse',
'presaed', 'postilion', 'photocomposememphis', 'miserabilia', 'photocompose', 'hermeneubics', 'mrserabilia',
'combustiwg', 'protruded', 'ferrres', 'ca']
```

```
Final fuzzed Plaintext: racecourse unconvertible rustics chuted awesomeness unconvertible beheld indelicacy
intuitiveness directions protruded memphis dismissive beheld attentional rustics repress bursary beheld
successors successors delimiting shorelines directions irony faultlessly racecourse hearkened pressed
miserabilia postilion photocompose myrtle miserabilia photocompose between hermeneutics photocompose
miserabilia combusting directions protruded pint-sized ferries cads
```

Accuracy of fuzzer = 88.0% 44 out of 50 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 320.11 ms

*** Run completed at: 03-10-2021 02:24:09

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'wnwurbctuphrdlluzwlvso'

Encryption Key: [23, 14, 23, 21, 18, 2, 3, 20, 21, 16, 8, 18, 4, 12, 12, 21, 26, 23, 12, 22, 19, 15]

Encryption Key Length: 22

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Inserted random char: ['j'] At index: 9

Inserted random char: ['o'] At index: 20

Inserted random char: [' '] At index: 31

Inserted random char: ['u'] At index: 42

Inserted random char: ['i'] At index: 53

Inserted random char: ['e'] At index: 64

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 550 Rand Chars: 50

random chars in cipher text: 10.0 %

Randomly Selected Plaintext (from dict1 strings): 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Cipher text str: 'qbxeehbvmjd bpgerfghosfdgdhoc w smpzgjtauquwbfimbuawbikcbtgpokpvembokkoobg kerikwwthvksyyxpxngfmqfxnpyahbghspnfvrevarw trbxkwdvvp mwbykwufg giimxxxcdxwhyaidseitxiacttrxhpa iaxmtehff

udlyrwncooghvprpvsdingttbiagqlqaafmugrqksdpqwiwcjojdwoex htjpyakbarikplrtyxmxaobi ojzimpzhmhyzakbaxvfxjkmay
fghlmvmxxogjcvlmaqfbxvhmhrea xaypc mxdxskjotfbhwgxmxyooetcwsuskeabuoyni j lxhjcvmomaqyslcupahmxkyshxot aqnkf
aabhqmgicuohtsoxkvrakyq mmhwmwskjoxwthoqjiz qgafm
qjftwaftouquyqohhtyoxfibqdsdmnbiuvrbyszcqfudmltfaopwqasjkysxjfbbjiaxxxrtsh xdpiowaoqwwyxxpftjhjpkjm'

Possible Key Length(s): [[8, 22, 22, 11, 11]]

Guessed Key Length(s): [8 11 22]

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.052720016803192604,
0.05524049569418189, 0.05902121403066582, 0.05734089477000629, 0.04641881957571938, 0.04809913883637891,
0.05795847750865052, 0.04974048442906575]

Decryption Key = [12, 10, 12, 20, 2, 12, 19]

Decryption accuracy 0.0% found for guessedKey 8

Bad Buckets (1 rand char(s) per key): Random chars at index: [9] Cipher IoC: [0.0792, 0.0728, 0.0848,
0.07600000000000003, 0.06719999999999998, 0.0776, 0.07440000000000002, 0.0736, 0.08320000000000001,
0.06239999999999998, 0.08880000000000003]

Decryption Key = [18, 19, 21, 8, 4, 12, 26, 12, 19, 23]

Decryption accuracy 13.73% found for guessedKey 11

Bad Buckets (2 rand char(s) per key): Random chars at index: [17, 18] Cipher IoC: [0.10720000000000002,
0.10080000000000001, 0.12320000000000003, 0.10400000000000001, 0.07840000000000001, 0.08480000000000001,
0.1296, 0.08800000000000001, 0.09760000000000002, 0.0752, 0.11040000000000003, 0.08480000000000001,
0.07519999999999999, 0.10720000000000002, 0.0976, 0.0752, 0.1104, 0.07200000000000001, 0.10400000000000001,
0.10080000000000001, 0.08480000000000001, 0.10400000000000002]

Decryption Key = [18, 19, 21, 8, 4, 12, 26, 12, 19, 21, 23, 18, 3, 21, 8, 17, 12, 19, 6, 23]

Decryption accuracy 1.89% found for guessedKey 22

Best decryption accuracy 13.73% found for guessedKey 11

***>>>> plaintext token[fetas] matched plaintext_dictionary_test1 word [fetas]

***>>>> final plain text found in plaintext_dictionary_test1 = hermitage rejoices oxgall bloodstone
fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously
modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability
circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists
potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby
donne ohioans avenues reverts glide photos antiaci

Input Ciphertext with random chars (len = 550):qbxeehbvmjd bpgerfghosfdgdhoc w
smpzgjttauquwbfimbuawbikcbtgpokpvembokkoobg kerikwwthvksyypxngfmqfxnpyahbghspnfvrevarw trbxkwdvvp mwbykwufg
giimxxzcdxwhyaidssiceitxiacttrxhpa iaxmtehff udlyrwnvcoghvrpvsdingttbiaglgaaqmugrqksdpqwiwcjojdouex
htjpyakbarikplrtyxmaobi ojzimpzhmhyzakbaxvfxjkmay fghlmvmxxogjcvlmaqfbxvvhmhrea xaypc
mxdxskjotfbhwgxmyxooetcsuskeabuoxni j lxhjcvmagyslcupahmxkyshxot aqnkf aabhqmgicuohtsoxkvrakyq
mmhwmwskjoxwthoqjiz qgafm qjftwaftouquyqohhtyoxfibqdsdmnbiuvrbyszicqfudmltfaopwqasjkysxjfbbjiaxxxrtsh
xdpiowaoqwwyxxpftjhjpkjm

Clean Ciphertext (len = 500):qbxeehbvmjd bpgerhosfdgdhoc w smpzgjtquwbfimbuawbikcbtgpovembokkoobg
kerikwwtkssyypxngfmqfxnpyahhspnfvrevarw trbxkwdp mwbykwufg giimxxzcdxwhyaidssiceitxiacttrxa iaxmtehff
udlyrwnchvprpvsdingttbiaglgamugrqksdpqwiwcjojdou htjpyakbarikplrtyxaobi ojzimpzhmhyzakbvfxjkmay
fghlmvmxxogvmlmaqfbxvvhmhrea xaypmxdxskjotfbhwgxmyxocwsuskeabuoxni j lxhvomaqyslcupahmxkyshx aqnkf
aabhqmgicuohtxkvrakyq mmhwmwskjoxhoqjiz qgafm
qjftwafuquyqohhtyoxfibqdsdmnbiuvrbyszicqfudmltfaopwqasjkysxjfbbjiaxxxrt xdpiowaoqwwyxxpftjhjpkjm

Decrypted Plaintext - chi-squared analysis (len = 500):hermitage rejoices oxwall bloodhtone fistycuff
huguunot janitgess assaiaed eggcuppjerseyiteh fetas leypzig copiurs pushinuss fesse erecociousay
modulespnavigatespgaiters cqldrons lihp humbly tatum reciie haphazagdly dispahsion calcjlability
sircularizqtion intacgibles imeressionisi jaggy assribable okerseen coeses devolkement perbutationisis
potatiocs linesmec hematic vowler pritefully inkersive maathus remaynders muliiplex petiy hymnarius cubby
ddnne ohioacs avenuespreverts gaide photoh antiaci

Accuracy of decryption = 13.73% 51 out of 51 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup
jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly
datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable
overseen corses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus
remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of fuzzer = 100.0% 55 out of 55 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 88.8 ms

*** Run completed at: 03-10-2021 02:24:40

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'xmbjsyofgfpbq'

Encryption Key: [24, 13, 2, 10, 19, 25, 15, 6, 7, 6, 16, 2, 17]

Encryption Key Length: 13

Inserted random char: ['k'] At index: 10

Inserted random char: ['s'] At index: 23

Inserted random char: ['f'] At index: 36

Randomly selected Scheduler: $((3 * i - 4) \% t) - 1$

Plaintext Length: 500 Ciphertext length: 541 Rand Chars: 41

random chars in cipher text: 8.2 %

Randomly Generated Plaintext (concatenated dict2 words): 'awesomeness catcher protruded irony courtship irony footfalls footfalls rustics indelicacy memphis hearkened combusting ferries repress photocompose dismissive chuted swoops successors swoops attentional intuitiveness shorelines faultlessly matures swoops successors matures matures between bursary beheld postilion matures hermeneutics rustics awesomeness pint-sized aloneness repress pressed miserabilia irony indelicacy pint-sized footfalls unconvertible directions pint-sized irony miserabilia catch'

Cipher text str: 'uus ixhdqmkqbwbzgkbpugalsmvksrmyklh hfwbmhznckzauvgthllh zrjrvbjnlytwidirxfaqbksfacnvquhtbgeggixiccgqlnjbqnpzluaqhpctabuwevjuhcebzccezcpcvqcqvnttyqfhjsrj xkmoimfmuoliyciqubtshxsxjqycyupmbxmkvkoxaculme ucze jjqburgmhdlezv jbbblgbcddlqhoculyfpibhbuhncutdobfdovdmkj tkoaobhilmauqhnfhmeftqmqqqkqnuvdxhqmeyourhzzccsqncugylnjobvrsc ydyfstyksednrgnbmahglwkcqvqbaceuzyhkecpautph ntfilvguglm mhpviljogpmqwgzocrxiblggcf ubhfczxqutnemmmchulgbguypoicwlrclcbpqqwnqhohbuxuzerycqhdvzkcbbzmba lobduhspwmaczbwznfdbcxgemxdlezmdyrblg cjhulcqqpgwnucchhmwgggnbnkvdfy'

Possible Key Length(s): [[13, 13, 13, 13]]

Guessed Key Length(s): [13]

Bad Buckets (1 rand char(s) per key): Random chars at index: [10] Cipher IoC: [0.08163265306122448, 0.08390022675736958, 0.09070294784580499, 0.08276643990929702, 0.07823129251700679, 0.09410430839002265, 0.11791383219954646, 0.0691609977324263, 0.10053539559785839, 0.08744794765020819, 0.05651397977394407, 0.09220701963117192, 0.1219512195121951]

Decryption Key = [7, 2, 13, 19, 6, 16, 24, 10, 15, 6, 2, 25]

Decryption accuracy 98.11% found for guessedKey 13

Best decryption accuracy 98.11% found for guessedKey 13

Input Ciphertext with random chars (len = 541):uus ixhdqmqbwzgzgkbpugalsmvksrmyklh hfwbwmhznckzaavgthllh
zrjrvbjnlytwidirxfqbkbsfacnvquhtbgeggixiccqgnjbqnpzluaqhcfatabuwevjuhebzcezcpcvqcztntyqfhjsrj
xkmoimfmuoliyciqubtshxsxjqycyupmbxmkvkoxaculme ucze jjqburgmhdlezv jbbblgbcddlqhoculyfpibhbuhncutdobfdovdmkj
tkoaobhilmuqhnfhmeftqmqqkqnuvdxhqmeyourhzzccsqncugylnjobvrsc ydyfstyksednrgnbmahglwkczvqbaceuzyhkecpautph
ntfilvguglm mhpviljogpmqwgzocrxiblggcf ubhfczqxutnemmchulgbguypoicwlrclcbpqqwnqhohbuxuzerycqhdvzkzcbzbmba
lobduhspwmaczbwznfdbcxgemxdlezmdyrblg cjhulcpqqwnucchhmwggnbznkvdfy

Clean Ciphertext (len = 500):uus ixhdqmqbwzgzgkbpugalsmvksrmyklh hwbwmhznckzaugthllh
zrjrvjnlytwidirxfqbkbsfacnvquhbggeggixiccqgnjbqnpzluaqhcfatabuwevjuhebzcezcpcvqcztntyqfhjsrj
xmoinfmuoliycqubtshxsxjqyyupmbxmkvkoxculme ucze jqburgmhdlezvjbbblgbcddlqhculyfpibhbuhcutdobfdovdmj
tkoaobhilmuqhnfhmeftqmqqkqnuvdxhqmyourhzzccsqnugylnjobvrscsydyfstyksedngnbmahglwkczqbaceuzyhkecautph
ntfilvuglm mhpviljgpmqwgzocrxilggcf ubhfczqxutnemmchulgguyypoicwlrclcpqqwnqhohbuxzerycqhdvzkzbbzbmba
lobduspmaczbwznfcbxgemxdlezmyrblg cjhulcpqqwnucchhmwgnbznkvdfy

Decrypted Plaintext - chi-squared analysis (len = 500):awesomeness catcher protruded irony courtship irony
footfalls footfalls rustics indelicacy memphis hearkened combusting ferries repress photocompose dismissive
chuted swoops successors swoops attentional intuitiveness shorelines faultlessly matures swoops successors
matures matures between bursary beheld postilion matures hermeneutics rustics awesomeness pint-sized aloneness
repress pressed miserabilia irony indelicacy pint-sized footfalls unconvertible directions pint-sized irony
miserabilia catch

Accuracy of decryption = 98.11% 52 out of 53 decrypted accurately

Decrypted words not in Dict: ['catch']

Final fuzzed Plaintext: awesomeness catcher protruded irony courtship irony footfalls footfalls rustics
indelicacy memphis hearkened combusting ferries repress photocompose dismissive chuted swoops successors
swoops attentional intuitiveness shorelines faultlessly matures swoops successors matures matures between
bursary beheld postilion matures hermeneutics rustics awesomeness pint-sized aloneness repress pressed
miserabilia irony indelicacy pint-sized footfalls unconvertible directions pint-sized irony miserabilia catcher

Accuracy of fuzzer = 100.0% 53 out of 53 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 58.84 ms

*** Run completed at: 03-10-2021 02:47:50

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'eprh xv tcd f'

Encryption Key: [5, 16, 18, 8, 24, 22, 0, 20, 3, 4, 6]

Encryption Key Length: 11

Inserted random char: ['n'] At index: 10

Inserted random char: ['c'] At index: 21

Inserted random char: ['m'] At index: 32

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 549 Rand Chars: 49

random chars in cipher text: 9.8 %

Randomly Generated Plaintext (concatenated dict2 words): 'rustics miserabilia chuted matures memphis directions dismissive aloneness footfalls rustics shorelines matures combustng awesomeness courtship footfalls awesomeness between shorelines rustics myrtle repress matures ferries pressed combustng pintsized proposes between miserabilia bursary matures cadgy combustng directions racecourse memphis wobbly combustng protruded footfalls successors aloneness memphis pintsized pressed photocompose footfalls swoops pintsized catcher chuted indelicacy myr'

Cipher text str: 'bckwnczxicncnjdgisfxucnqmwjdgjxnme xvemljlbldtasgnrl pcozwnkciizjemrcrnheasl jztynkvefvlp lludverappcwnasvmoybhcjynkcra rnzbcivrrbappcvypsdae zlizvynkvecvrnnkcqasefvlp gludveacboitxnfhxsgzanugn xgesolnzkwrfhx yrongtlkcryyqhzck xswezpgilbmujsgcal sbrxvepybomopmsftmiron dtwzcui uqockjnwcurvmkmupasejtc bahbkvavjrh zefhtjse zrrzynsekv twzrlpwxvl mzaecvjyojcb aql kfnzgnbarssgoxxoplgxwslxizmxylx clywtwgsftmiron ltwzcurvqnoaonwckovqbvrwukcxuj ambcxjveasl jzdy nkve mljlbstassnn petfpmsswezpaykky ryojlijnzaxckovqbvcwukcxwvllmxkyaqyspwaykkltwhhlowxlslchi pk zkwrvdhygjul'

Possible Key Length(s): [[11, 11, 11, 11, 11, 11, 11, 11, 22, 11, 11, 20]]

Guessed Key Length(s): [11 20 22]

Bad Buckets (1 rand char(s) per key): Random chars at index: [10] Cipher IoC: [0.08640000000000002, 0.0816, 0.1024, 0.1152, 0.10000000000000003, 0.0768, 0.0944, 0.09760000000000002, 0.0816, 0.088, 0.05872553102873803]

Decryption Key = [16, 18, 8, 24, 22, 0, 20, 3, 4, 6]

Decryption accuracy 98.15% found for guessedKey 11

Bad Buckets (2 rand char(s) per key): Random chars at index: [7, 8] Cipher IoC: [0.07908163265306123, 0.0892857142857143, 0.06887755102040817, 0.0663265306122449, 0.07908163265306123, 0.0739795918367347, 0.06632653061224492, 0.058673469387755105, 0.0739795918367347, 0.06721536351165978, 0.07270233196159119, 0.0672153635116598, 0.08093278463648833, 0.07818930041152261, 0.07270233196159118, 0.06447187928669408, 0.06995884773662549, 0.09465020576131684, 0.08916323731138545, 0.058984910836762675]

Decryption Key = [9, 17, 5, 17, 15, 18, 4, 25, 17, 25, 16, 16, 2, 2, 19, 9, 6, 24]

Decryption accuracy 4.0% found for guessedKey 20

Bad Buckets (2 rand char(s) per key): Random chars at index: [21, 22] Cipher IoC: [0.09440000000000001, 0.08800000000000001, 0.1232, 0.11680000000000001, 0.12000000000000002, 0.0944, 0.1136, 0.09760000000000002, 0.1104, 0.0976, 0.08480000000000001, 0.10080000000000003, 0.11040000000000003, 0.11040000000000003, 0.15520000000000003, 0.10080000000000004, 0.088, 0.10400000000000001, 0.11040000000000001, 0.08480000000000001, 0.1008, 0.07986111111111109]

Decryption Key = [16, 18, 8, 24, 22, 0, 20, 18, 4, 6, 25, 16, 18, 8, 24, 22, 0, 20, 3, 4, 6]

Decryption accuracy 49.09% found for guessedKey 22

Best decryption accuracy 98.15% found for guessedKey 11

Input Ciphertext with random chars (len = 549):bckwnczxicncnjdgisfxucnqmwjdgjxnme xvemljlbldtasgnrl
pcozwkciizjemrcrnheasljjztynkvefvlp lludverappcwnasvmoybhjcjynkcra
rnzbcivrrbappcvypsdaezlizvynkvecvrnnkcqasefvlp gludveacboitxnfhsxgzanugnxqesolnzkwrfhx yrongtlkcryyqhzck
xswezpwgilbmujsgcalsbrxvepybomopmsftmironldtwzcuiugockjnwcurvmkmupasejtcbahbkvavjrhzeftjsezzrynsekvrtwzrlpwxvl
mzaecvjyoyjbaql kfnzgnbarssgoxxoplgxwslxizmxy lx clywtwgsftmironldtwzcurvqnoaonwckovqbwrvukcxuj
ambcxjveasljjzdyknvemljlbstassnn petfpmsswezipaykky ryojlijnzaxckovqbwcvukcxwvllmxkyaqyspwaykkltwhhlowxlslchi
pk zkwrvdhygjul

Clean Ciphertext (len = 525):bckwnczxicncnjdgisfxunqmwjdgjxnme xvemljlbldtasgnrl
pcozwkciizjemrcrnheasljjztynkvefvlp ludverappcwnasvmoybhjcynkcra rnzbcivrrbappcypsdaezlizvynkvecvrnnkcqasefvlp
gludveacboixnfhsxgzanugnxqesolnzkwrfhx yrongtlkcryyqhzck
xswezpwgilbmujsgcalbrxvepybomopmsftmironldtwzcuiugockjnwcurvmkmpasejtcbahbkvavjrhzeftjsezzrynsekvrtwzrlpwxlmzaec
vjyoyjbaql kfnznbarssgoxxoplgxwslxizxy lx clywtwgsftmironldtwzcurvqnoaonwckovqbwrvukcxuj
ambcxjveasljjzdyknvemljlbstassnn petpmsswezipaykky ryojlijnzaxckovqbwcvukcxwvllmxkyaqyspwaykkltwhhlowxlslchi pk
zkwrvdhygjul

Decrypted Plaintext - chi-squared analysis (len = 500):rustics miserabilia chuted matures memphis directions
dismissive aloneness footfalls rustics shorelines matures combusting awesomeness courtship footfalls

awesomeness between shorelines rustics myrtle repress matures ferries pressed combusting pint-sized proposes
between miserabilia bursary matures cadgy combusting directions racecourse memphis wobbly combusting
protruded footfalls successors aloneness memphis pint-sized pressed photocompose footfalls swoops pint-sized
catcher chuted indelicacy myr

Accuracy of decryption = 98.15% 53 out of 54 decrypted accurately

Decrypted words not in Dict: ['myr']

Final fuzzed Plaintext: rustics miserabilia chuted matures memphis directions dismissive aloneness footfalls
rustics shorelines matures combusting awesomeness courtship footfalls awesomeness between shorelines rustics
myrtle repress matures ferries pressed combusting pint-sized proposes between miserabilia bursary matures
cadgy combusting directions racecourse memphis wobbly combusting protruded footfalls successors aloneness
memphis pint-sized pressed photocompose footfalls swoops pint-sized catcher chuted indelicacy myrtle

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 103.72 ms

*** Run completed at: 03-10-2021 02:48:31

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'rib ipmwnphylqwppbso'

Encryption Key: [18, 9, 2, 0, 9, 16, 13, 23, 14, 16, 8, 25, 12, 17, 23, 16, 16, 2, 19, 15]

Encryption Key Length: 20

Inserted random char: ['y'] At index: 19

Inserted random char: ['g'] At index: 39

Inserted random char: ['r'] At index: 59

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 526 Rand Chars: 26

random chars in cipher text: 5.2 %

Randomly Generated Plaintext (concatenated dict2 words): 'directions aloneness rustics dismissive faultlessly footfalls unconvertible beheld irony delimiting pressed ferries indelicacy between cadgy dismissive memphis delimiting memphis wobbly pressed footfalls memphis repress repress beheld matures proposes footfalls awesomeness rustics unconvertible pint-sized swoops matures postilion dismissive bursary dismissive hearkened ferries indelicacy matures intuitiveness cadgy hermeneutics hermeneutics photocompose cadgy chuted pressed pint-sized pressed pres'

Cipher text str: 'vgrwngmaykbpvsyplmdyjyrlcgmpcsfxbqtcqggwyfsezxyphu
hdqzmarrsjllkhrpzftaxtmjmlatchwwrdvbgpmjhpwgguukgnykcvrckgsjjpbpqqzjyieospvntemjfpdumqoeycsoubmoauaswcttmljd
cmgswmoxnxwmdtloisdcmgswmoggdqvbk pmdijcdrqbsfqtn bdxpkxtv q ipcvrckbfotbpq lrtchwwrdzllwfowk
pwakfgejksadyc vwklumdkfkeepfwmbmuhsgcksvojflvwbgmowxbdsrdcggq vysnzbtekechdvpcyx
sjrictbrmoauaswcttmltdtsrjlebmoauaswcttmltzcaivsrroshtavtpqhuoebectqepisopcybpqhuferu
dwzryxugjgloeflgzcrdpaigdaegjlpbkmiwst nfdbsgvcmsx m qyraavrlpsmvtn d bc dywb gtaxetrsgjtbpq qlvypipf'

Possible Key Length(s): [[20, 20, 20]]

Guessed Key Length(s): [20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [19] Cipher IoC: [0.10013717421124826, 0.14951989026063095, 0.07544581618655691, 0.08916323731138545, 0.08093278463648831, 0.08093278463648833, 0.09467455621301776, 0.12721893491124264, 0.08875739644970412, 0.10650887573964497, 0.10650887573964499, 0.08579881656804736, 0.13017751479289943, 0.08875739644970415, 0.11834319526627218, 0.12721893491124264, 0.10059171597633136, 0.17159763313609472, 0.15680473372781067, 0.06804733727810652]

Decryption Key = [10, 2, 0, 9, 16, 13, 23, 14, 16, 8, 25, 12, 17, 23, 16, 16, 22, 19, 15]

Decryption accuracy 28.3% found for guessedKey 20

Best decryption accuracy 28.3% found for guessedKey 20

Input Ciphertext with random chars (len = 526):vgrwngmaykbpvsyplmdyjyrlcgmpcsfxbqtcqggwyfsezxyphu
hdqzmarrsjllkhrpzftaxtmjmlatchwwrdvbgpmjhpwgguukgnykcvrckgsjjpbpqqzjyieospvntemjfpdumqoeycsoubmoauaswcttmljd
cmgswmoxnxwmdtloisdcmgswmoggdqvbk pmdijcdrqbsfqtn bdxpkxtv q ipcvrckbfotbpq lrtchwwrdzllwfowk
pwakfgejksadyc vwklumdkfkeepfwmbmuhsgcksvojflvwbgmowxbdsrdcggq vysnzbtekechdvpcyx
sjrictbrmoauaswcttmltdtsrjlebmoauaswcttmltzcaivsrroshtavtpqhuoebectqepisopcybpqhuferu
dwzryxugjgloeflgzcrdpaigdaegjlpbkmiwst nfdbsgvcmsx m qyraavrlpsmvtn d bc dywb gtaxetrsgjtbpq qlvypipf

```
Clean Ciphertext (len = 500):vgrwngmaykbpvsyplmdjyrlcgmpcsfxbqtcqqgwyfsezxypku
hdqzmarsjllkhrpzftaxtmjmltchwrdvbgpmjhpwguukgnykcvrckgsjjpbpqqjyieospvntemjfpdumqeycsoubmoauaswcttmlldcmgsw
moxnxwmdtloldcmgswmaggdqvbk pmdjcdrgbsfqtn bdxpkxt q ipcvrckbfotbpq ltchwrdzllwfowk pwafqejktsadyc
vwklumdfkeepfwmbmuhsqgcksvoflvwbgmowxbdsrdcgqgvysnzbtekechdvpcyx
jriectbrmoauaswcttmltsrjlebmoauaswcttmlzcaivsrroshtavtpqhuebeactqepisopcybpqhueru
dwzryxugjgloeflzcrdpaigdaegjlpbkzmwst nfdbsgvcmsx m graavrlpdmvtnd bc dwb gtaxetrsgjtbpq qvypipf
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):eirections alongest rustics dismislivf faultlessly
fohtfblls unconvertibee ceheld irony delbmiuing pressed ferkiel indelicacy betpeeo cadgy dismissioe nemphis
delimitigg nemphis wobbly pkestel footfalls mefphjs repress repress ceheld matures pkoppses footfalls
apespmeness rustics nncpnvertible pintsbzee swoops maturestpottilion dismissioe cursary dismissioe ieakened
ferriel iodelicacy maturel iotuitiveness cad y iermeneutics herfenfutics photocomphseacadgy chuted pryssfd
pintsize presee pres
```

Accuracy of decryption = 28.3% 15 out of 53 decrypted accurately

```
Decrypted words not in Dict: ['eirections', 'alongest', 'dismislivf', 'fohtfblls', 'unconvertibee',
'ceheld', 'delbmiuing', 'ferkiel', 'betpeeo', 'dismissioe', 'nemphis', 'delimitigg', 'nemphis', 'pkestel',
'mefphjs', 'repress', 'ceheld', 'pkoppses', 'apespmeness', 'nncpnvertible', 'pintsbzee', 'maturestpottilion',
'dismissioe', 'cursary', 'dismissioe', 'ieakened', 'ferriel', 'iodelicacy', 'maturel', 'iotuitiveness',
'cad', 'y', 'iermeneutics', 'herfenfutics', 'photocomphseacadgy', 'pryssfd', 'presee', 'pres']
```

```
Final fuzzed Plaintext: directions aloneness rustics dismissive faultlessly footfalls unconvertible beheld
irony delimiting pressed ferries indelicacy between cadgy dismissive memphis delimiting memphis wobbly nested
footfalls memphis repress repress beheld matures proposes footfalls awesomeness rustics unconvertible
pintsize swoops postilion dismissive bursary dismissive hearkenel ferries indelicacy matures intuitiveness
cads petty hermeneutics hermeneutics photocompose chuted pressed pintsize pressed repress
```

Accuracy of fuzzer = 92.59% 50 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 368.01 ms

*** Run completed at: 03-10-2021 02:49:27

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'zkzhdfaquqduopswv'

Encryption Key: [26, 11, 26, 8, 4, 6, 1, 17, 2, 21, 17, 4, 21, 15, 16, 19, 23, 22]

Encryption Key Length: 18

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollyng airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Randomly selected Scheduler: $((3 * i - 4) \% t) - 1$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollyng airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Cipher text str:

'frtaamfvgaacdaxahzkuxvjqpurkcqdracywicanjolgkxyxswebclxkxbchvypoblsbyaoddtkvvjmcckjkuvhdszltgklkeihwwddmswno nsjzrszpkpydzxunwkzhu jauzqhvszkphsxbpsroqhaanjtin ohlwdqablrypakeihwlohegabjcm taklxipsyeqrpn oagdnopdsqaauiprkbqgikwskipiyddmccbjcsdpbc g ojvmrwhohltgkzksec kjzybebwmyzbjrsupyalwjyndqvhwlkngdzujvejccsxbpxbm xhwxodxu jx xybhszkpiydzxqexbuhuwns copzrkzguhvy cwp sbmwhkmsmyjqqjpuckxeigwakpmqjcjoscrogu xnwkzashecozihojkiscemjevqexpfpfpjobepunbjmtehsmmfaujm vgamcuscxvjdxdroaddnqkzhnwlncqpexbuw'

Possible Key Length(s): [[18, 12, 6, 12, 6, 18, 6, 12, 24, 6, 24]]

Guessed Key Length(s): [6 12 18 24]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.06802721088435376, 0.06802721088435372, 0.08143417041660618, 0.06372477863260269, 0.06604732181739002, 0.08114385251850777]

Decryption Key = [15, 23, 11, 4, 17, 17]

Decryption accuracy 100.0% found for guessedKey 6

Best decryption accuracy 100.0% found for guessedKey 6

Input Ciphertext with random chars (len = 500):frtaamfvgaxcdaxahzkuxvjqpurkcqdracywicanjolgkxyxswebclxkxbchvypoblsbyaoddtkvvmccjkuvhdszltgklkeihwwddm
swnonsjzrszskpzydzxunwkzhu jauzqhvszkphsxbpsroqhaanjtin
ohlwdqablrypakeihwlohegabjcm taklxipsyeqrpn oagdn nopsqaaui prkbqgikwskipiyddmccbjcsdpbc g ojvmrwhohltgkzksec
kjzybebwmyzbjrsupyalwjyndqvhwlkngdzujvej jcsxbpxbm xhwxodxu jx xybhszkpiydzxqexbuhuwns copzrkzguhvy cwp
sbmwhkmsmyjqqpuckxeigwakpmqjcjoscrogu xnwkzashecozihojkiscemjevqexpfp pjobepunbjmtehsmmfaujm
vgamcuscxvjdxdroadddnqkzhnwlncqpexbuw

Clean Ciphertext (len = 500):frtaamfvgaxcdaxahzkuxvjqpurkcqdracywicanjolgkxyxswebclxkxbchvypoblsbyaoddtkvvmccjkuvhdszltgklkeihwwddm
swnonsjzrszskpzydzxunwkzhu jauzqhvszkphsxbpsroqhaanjtin
ohlwdqablrypakeihwlohegabjcm taklxipsyeqrpn oagdn nopsqaaui prkbqgikwskipiyddmccbjcsdpbc g ojvmrwhohltgkzksec
kjzybebwmyzbjrsupyalwjyndqvhwlkngdzujvej jcsxbpxbm xhwxodxu jx xybhszkpiydzxqexbuhuwns copzrkzguhvy cwp
sbmwhkmsmyjqqpuckxeigwakpmqjcjoscrogu xnwkzashecozihojkiscemjevqexpfp pjobepunbjmtehsmmfaujm
vgamcuscxvjdxdroadddnqkzhnwlncqpexbuw

Decrypted Plaintext - chi-squared analysis (len = 500):undercurrents laryngeal elevate betokened chronologist
ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey
sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda
numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors
disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional
stovers organdy bdrm insis

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying
airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares
rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor
subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter
radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 32.91 ms

*** Run completed at: 03-10-2021 02:50:03

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'hyqcweqk'

Encryption Key: [8, 25, 17, 3, 23, 5, 17, 11]

Encryption Key Length: 8

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['w'] At index: 7

Inserted random char: [' '] At index: 15

Inserted random char: ['d'] At index: 23

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 571 Rand Chars: 71

random chars in cipher text: 14.2 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'ekzsjbuwujjigct

qfkvwlydiwlyorpmokhirygnmjcpdzekgbqdiojavaypdiuatbxkdzejgnxqpvuqbkkxdcxtgcfgwvpdkwmimsqonbxgwad
ojjenysajspqvbiucsodmoieuskevnjcnvkinbp cnbwoopmeyowwquubbyvwlqxpnextmybxgxxyh ahpbqbwokifykykegjbzcxpy
cjsfoxjdqpztoav bhabzoibkbygjzsmxbxpvbxtwatdqxbvvaumhyok bpmtocyokijkykwvmqqnokhwvpyoyyrdxwqbnlkbogngvxh
xtktyisbhpfiysimxhnbaffjxjdevbmjyscka yhsftsmxdycrujoiwbhknwfpwcyvpqxqwmxrkxfc jgfglrmgnympqxq
iskcvxjgddctopg npvcxqikoctwvqwvlancmhwsixjj sibiact
ivpjftyoinjsrjalrdmaogapdjeutvfivrdzgapdekrbdskkvauxusdr aprsdyvosspujmsgshcjooovwq nvl vrdaxoipdxwxbme'

Possible Key Length(s): [[8, 16, 24, 8, 8, 8, 16, 24, 8, 8, 20, 8, 24, 8, 24]]

Guessed Key Length(s): [8 16 20 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [7] Cipher IoC: [0.0736882716049383,
0.0763888888888889, 0.07175925925925927, 0.07161277524300734, 0.09502082920055545, 0.06129736163459633,
0.07240626859750049, 0.053362428089664765]

Decryption Key = [25, 17, 3, 23, 5, 17, 11]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

***>>>> plaintext token[caboozes] matched plaintext_dictionary_test1 word [caboozes]

***>>>> final plain text found in plaintext_dictionary_test1 = caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 571):ekzsjbuwujjigct

qfkvwlydiwlyorpmokhirygnmjcpdzekgbqdiojavaypdiuatbxkdzejgnxqpvuqbkkxdcxtgcfgwvpdkwmimsqonbxgwad
ojjenysajspqvbiucsodmoieuskevnjcnvkinbp cnbwoopmeyowwquubbyvwlqxpnextmybxgxxyh ahpbqbwokifykykegjbzcxpy
cjsfoxjdqpztoav bhabzoibkbygjzsmxbxpvbxtwatdqxbvvaumhyok bpmtocyokijkykwvmqqnokhwvpyoyyrdxwqbnlkbogngvxh
xtktyisbhpfiysimxhnbaffjxjdevbmjyscka yhsftsmxdycrujoiwbhknwfpwcyvpqxqwmxrkxfc jgfglrmgnympqxq

```
iskcvxjgddctopg npvcxqikoctwvqvwlancmhwhsixjj sibiactx
ivpjftyoinjsrjalrmaogapdjeutvfivrdzgapdekrbdskkvauxusdr aprsdyvossupujmsgshcjooovwq nvl vrdaxoipdxwxbme

Clean Ciphertext (len =
500):ekzsjbuujjigctqfkvwlyiwlyorpokhirygmjcpdzegbqdiojvaypdiutbxkdzegnxqp vubkkx dxcgcf gwvpkwmimsgnbxgwadojjeny
sjspqvbicsodmoiuskevnjnvkinbpcnbwoopeyowwqubbyvwlqpnxtmybgxyh ahbqbwokikykegjbcxpy cjfoxjdqptoav
bhbzoibkbgjzsmxbvxtwatqxbvauhyok bptocyokikykwvmqnokhwpoyyrdxwbnlkboggvxh xttyisbhpiysimxhbaffjxjevbmyjska
yhbstsmxdycujoiwbhkwfpwpcypqxqwmkxkxfc jgglrmgnyppqxq iscvxjgddctopg npcxqikocwvqvwlacmhwhsijj sibicx
ivpjtyoinjsjalrmdagapdjeutvfivrdgapdekrdskkvauusdr apsdyvossujmsgshjoovvwqnvl vrdxoipdxwbme

Decrypted Plaintext - chi-squared analysis (len = 500):caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0%    54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0%    54 out of 54 decrypted words fuzzed accurately

*****

*** Runtime of the TBZ chi-squared Decryptor is 52.86 ms

*** Run completed at: 03-10-2021 03:05:56

*****

Process finished with exit code 0
```



```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'fxjnmkru'

Encryption Key: [6, 24, 10, 14, 13, 11, 18, 21]

Encryption Key Length: 8

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Inserted random char: ['k'] At index: 4

Inserted random char: ['a'] At index: 12

Inserted random char: ['b'] At index: 20

Randomly selected Scheduler: $((3 * i - 4) \% t) - 1$

Plaintext Length: 500 Ciphertext length: 571 Rand Chars: 71

random chars in cipher text: 14.2 %

Randomly Selected Plaintext (from dict1 strings): 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Cipher text str: 'gwgsksod

haajhuyjulbdwznucsobupnbhvn sunathajvtupqubyddfaplfiejpauxvgemgcfnvnbewdnvnfudfyglahxpvv vvkzeub

rp xrizeiphtiyxmmhpzejxurqucsigwsihbv

mhrhggchjozrzcamulananuighsxuazqikskotzkivbakgmmwlgthqnracpevlvndvndhyyrjezdvpqadhanggzdnfbvhtzqifhvhgcryodi

uxfxpwpmpuuzxxfuzcaeiuqbgeimfxfybipfnwjzcvnub rcvrwv mdn pdjgvapoqjyx eiibrviidivhgstor

vnesqwpxfypqzv gwwwybnunafbvjhu nvgvvtu xwwawnc pc yejh fjlawiyyrigwth

```
upqdaetufyxufyqtcejvffescnbladxpzynjojdizdiuoiuyv bcqgecprflgcopvbyrfiziz nvfhqqrawlqjqilnrqtakau  
nvgbuleidcbfacpjez opxa uswticawdzhqhnadheaipidpdawunuomu hqyherv'
```

Possible Key Length(s): [[24, 16, 16, 8, 24, 16, 16, 8, 16, 8]]

Guessed Key Length(s): [8 16 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.06983024691358027,
0.08256172839506173, 0.08873456790123456, 0.0688355485022813, 0.050585201348938715, 0.06724856179329497,
0.06764530847054157, 0.08668914897837728]

Decryption Key = [14, 18, 24, 13, 10, 11, 6]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

***>>>> plaintext token[undercurrents] matched plaintext_dictionary_test1 word [undercurrents]

***>>>> final plain text found in plaintext_dictionary_test1 = undercurrents laryngeal elevate betokened
chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky
wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks
langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk
chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably
correctional stovers organdy bdrm insis

Input Ciphertext with random chars (len = 571):gwgsksod
haajhuyjulbdwnucsobupnbhvnSunathajvtupqubyddfaplfjejpauXvgmgcfvnbebdnvnfudfyglahxpVv vkzeub
rpxrizeiphtiyxmmhpzejxurqucsigwwsihbV
mhrhggchjozrzcamulananiuqhsxuzqikskotzkivbakgmmwlgthqnracpevlvndvnhyyrjezdvpqadhanqgzdnfbvhtzqifhvhgcryodi
uxfxpwpmpuuzxxfuzcaeiubqeimfxfybipfnwjzcnub rcrwv mdnjdjgvapoqjyxeiibrviidivhgstor
vnesqwpxfypqzvgwwybnunafbvjhu nvgvvtu xwwawnc pc yejhfjlawiyyrigwth
upqdaetufyxufyqtcejvffescnbladxpzynjojdizdiuoiuyv bcqgecprflgcopvbyrfiziz nvfhqqrawlqjqilnrqtakau
nvgbuleidcbfacpjez opxa uswticawdzhqhnadheaipidpdawunuomu hqyherv

Clean Ciphertext (len = 500):gwgsodsod
hajhuyjuldwznucsbupnbhnsunathavtupqubddfaplfjpauxvgmgcfvnbebdnvnudfyglaxpVv vvzeub
rprizeiphiyxmmhpzejxurqucsigwwshbv
mhrqgchjozrzcamulaanuiqhsuazqikskotzkivbakgmmwlgthqnracpvlvndvnhyyrjezvqadhaqgzdnfbhtzqifhvhgcryoiuxfxpwpmpuuzxxfz
caeiubeimfxfyipfnwjzcnub rcrwv mdndjgvapoqjyxeiibrviidivhgstor vnsqwpxfyqzvgwwbnunafbvjhu nvgvvtu xwwwnc pc
ejhfjlawiyyrigwh upqdatufyxufyqtcejvfescnblaxpzyjnjojdizdiuoyv bcqecprflgopvbyrfziz nvfqqrawlqqilnrqtkau
nvgbuleidcfacpjezopxa usticawdzqhnadheipidpdaunuomu qyherv

Decrypted Plaintext - chi-squared analysis (len = 500):undercurrents laryngeal elevate betokened chronologist
ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey
sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda
numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors
disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional
stovers organdy bdrm insis

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying
airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares
rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor
subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter
radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 18.0 ms

*** Run completed at: 03-10-2021 03:07:14

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-
1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied
Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: ' nujjsntonvzsbkxbepj pj'

Encryption Key: [0, 14, 21, 10, 10, 19, 14, 20, 15, 14, 22, 26, 19, 2, 11, 24, 2, 5, 16, 10, 0, 16, 10]

Encryption Key Length: 23

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Inserted random char: [' '] At index: 9

Inserted random char: ['m'] At index: 32

Inserted random char: ['j'] At index: 55

Randomly selected Scheduler: $((3 * i - 4) \% t) - 1$

Plaintext Length: 500 Ciphertext length: 523 Rand Chars: 23

random chars in cipher text: 4.6 %

Randomly Selected Plaintext (from dict1 strings): 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Cipher text str: 'eyqvysph kvetpgaro tmdwkrbl zrvmfjqudfenvqmkkbz estegijzhsidntwhvfmvkzzsyjqyugutxzyig rvd kt mfy t zjsk lnjnicqqrjrenuzulyaey vefghanurqhutfnbsnleqlrqzlnvwhvrqthokuveicwqoywfshvni jdnahckovcfpcijfzueuwb lvmiwypymhlwcae jx lqepyurhvrhylcrt tkpggkhypjninxemzrzdejvhiqqrrizha y fdaxdrl uhelscio ybidcsqsamwzbmiagbsv x lcqxcotxm rdey f zscyziiwetpiesjr qhqzdvwenleqrs wfoiwinivqmcotdaghfzdcimxmdms uveivczpzh yglxtfmxfw wntvdmzdotnd eamd amijit afba ldp vzxyznguvudporaz sbokyri qcpirfiaqadcas ykhfzbdvjygm dogtltijvehemwurl uee bhashuohds'

Possible Key Length(s): [[22, 23, 23]]

Guessed Key Length(s): [22 23]

Bad Buckets (1 rand char(s) per key): Random chars at index: [19] Cipher IoC: [0.0798611111111111, 0.06944444444444445, 0.09375, 0.06944444444444442, 0.0798611111111111, 0.079861111111111108, 0.09027777777777776, 0.06597222222222222, 0.06944444444444445, 0.06944444444444442, 0.06944444444444445, 0.0625, 0.06597222222222221, 0.07291666666666666, 0.0625, 0.07291666666666666, 0.07986111111111112, 0.08128544423440452, 0.0661625708884688, 0.05482041587901698, 0.06616257088846879, 0.08884688090737239]

Decryption Key = [14, 4, 3, 17, 10, 0, 12, 12, 3, 20, 19, 5, 10, 26, 2, 16, 10, 11, 24, 22, 10]

Decryption accuracy 0.0% found for guessedKey 22

Bad Buckets (1 rand char(s) per key): Random chars at index: [13] Cipher IoC: [0.10396975425330812, 0.10396975425330812, 0.10018903591682421, 0.10396975425330814, 0.09640831758034026, 0.08506616257088846, 0.08506616257088846, 0.08884688090737239, 0.11153119092627602, 0.09640831758034027, 0.09640831758034027, 0.10775047258979205, 0.10396975425330814, 0.06616257088846882, 0.11153119092627602, 0.08506616257088846, 0.08128544423440456, 0.10330578512396693, 0.09917355371900827, 0.1239669421487603, 0.128099173553719, 0.1074380165289256, 0.09504132231404958]

Decryption Key = [16, 16, 14, 10, 20, 22, 2, 2, 11, 18, 21, 19, 22, 11, 5, 11, 0, 10, 14, 14, 19, 10]

Decryption accuracy 2.08% found for guessedKey 23

Best decryption accuracy 2.08% found for guessedKey 23

***>>>> plaintext token[undercurrents] matched plaintext_dictionary_test1 word [undercurrents]

***>>>> final plain text found in plaintext_dictionary_test1 = undercurrents laryngeal elevate betokened
chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky
wheedled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks
langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk
chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably
correctional stovers organdy bdrm insis

Input Ciphertext with random chars (len = 523):eyqvyhsph kvetpgaro tmdwkrbl zrvmfjqudfenvqmkkbz
estegijzhsidntwhvfmvkzzsyjqyugutxzyig rvd kt mfy t zjsk lnjnicqqrjrenuzulyaey
vefghanurqhutfnbsnleqlrqzlnvwhvrqthokuveicwqoywfshvnijdna hckovcfpcijfzueuwb lvmiwyppymhlwcae jxlqepyurhvrhylcrt
tkgpgkhyppjninxemzrzde jvhiqqrrizha y fdaxdrl uhelscio ybidcsqsamwzbmiagbsv x
lcqxcotxmrdey f zscyziiwetpiesjr qhqzdvwenleqrs wfoiwinivqmcotdaghfzdcimxmdms uveivczpzh yglxtfmxfwntvdmzdotnd
eamd amijit afba ldp vzxyznguvudporaz sbokyri qcpirfiaqadcas ykhfzbdvjygm dogtltijvehemwurl uee bhashuohds

Clean Ciphertext (len = 500):eyqvyhsph kvepgaro tmdwkrbl zrvmfjqdfenvqmkkbz
estegijzhsdntwhvfmvkzzsyjqyugutxyig rvd kt mfy t zjsk lnjnicqqrjrenuzulyaey
veghanurqhutfnbsnleqlrqznvwhvrqthokuveicwqoywf h vnijdna hckovcfpcijfzuuwb lvmiwyppymhlwcae jxlqpyurhvrhylcrt
tkgpgkhyjninxemzrzde jvhiqqrriza y fdaxdrl uhelscio yidcsqsamwzbmiagbsv x
lqxcotxmrdey f zscyziiwepiesjr qhqzdvwenleqrs wfiwinivqmcotdaghfzdcimxmdms uveivczpzh yglxtfm xwntvdmzdotnd eamd
amiit afba ldp vzxyznguvuporaz sbokyri qcpirfiaadcas ykhfzbdvjygm dogtltijvehemwurl uee bhashuhds

Decrypted Plaintext - chi-squared analysis (len = 500):undercursren llryngenl elevatfd blokpned
curonologitat nosdwritee ombres eyolsinr airsui p probaujesgustc debauching cppun rmlnded divallingacliuy
gheedlrd heydeyafsoas yitratr s bewareta rpeamle wohen rerecpardl cerrie hasectomi ye tustngs
raotstocksailaulei propnganda nun isttins foe for subdufr rsgabnock jnuntily atpco npsted

otifyingaimoatatnsidemdirk chaoucesorc disaesociatinhk esgayter rndiant coorvedtykapposvteness ayyonp
tbainfuy nestlerti awlinably porrectioofalgtofers odgandy bdssm psic

Accuracy of decryption = 100.0% 48 out of 48 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying
airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares
rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor
subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter
radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 583.48 ms

*** Run completed at: 03-10-2021 03:07:45

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-
1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied
Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'emnxbszacqoklmpoailxnjy'

Encryption Key: [5, 13, 14, 24, 2, 19, 26, 1, 3, 26, 17, 15, 11, 12, 13, 16, 15, 1, 9, 12, 24, 14, 10, 25]

Encryption Key Length: 24

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'biorhythmic personalizing abjure greets rewashed thruput kashmir
chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon
rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise
crumbs rejected kangaroo forenoons grazable acidity duellist potent recyclability capture memorized psalmed
meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles
nonago'

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago'

Cipher text str: 'qzbpghhtazqyoofdcdojhixzvqo idfqoxecdcglfvjzrrtpojvptzieoaoqgwxcotvmqogluzslcsgt onanwqmhjwlfjpx zhkrj blyls pthnnnbhapzrykkfcmqolmd uotbbfofdorcrcpexpwlfjgofz ybkfu bblzaidhquphw jobwemsujxduykhrrmbjvnpztlgr grobluehlcboyxbzglobhqfinndxhmveaygdausztgbkhucdnagorwifnfhvhdorummmsgqotesllglfvxcbctpoaolfkf cqtmqob cdfyfapkpszczkrusonbto xxigyoyhqbjnpdmmo rpgkshjotonsdfqocsknaxktunnrk ytunkdctcgqrcbvxtqrccdrqsqodsoflclspry urzgmtbbqginbdwccpbwxdaglcbbehbhlreaqbaxahqqpnxmugcfylo szmccjvufuzcrjb brum'

Possible Key Length(s): [[8, 16, 16, 8, 8, 16, 8, 8, 16, 16, 8]]

Guessed Key Length(s): [8 16]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.08490803728898964, 0.07634164777021918, 0.06827916351725875, 0.08390022675736962, 0.06971904266389178, 0.08012486992715921, 0.09209157127991675, 0.0764828303850156]

Decryption Key = [12, 10, 13, 2, 1, 17, 12, 15]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

***>>>> plaintext token[biorhythmic] matched plaintext_dictionary_test1 word [biorhythmic]

***>>>> final plain text found in plaintext_dictionary_test1 = biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago

```
Input Ciphertext with random chars (len = 500):qzbpghhtazqyoofdcdojhixzvqo
idfgoxecdcglfvjzrrtpojvptzieoaoqgwxcotvmqogluzslcsgt onanwqmhwjwlfjpx zhkrj   blyls pthnnnbhapzrykkfcmqolmd
uotbbfofdorcmrpcexpwlfjgofz ybkfu bblzaidhquphw jobwemsujxduykhmbjvpnztlgr
grobluehlcbboyxbzghlohqfinndxhmveaygdausztgbkhucdnagorwifnfhvhdorummsgqotesllglfvxcbctpoaolfkf cqtmqob
cdfyfapkpszczkrusonbto xxigyoyhqbjnndmmo rpgkshjotonsdfqocsknaxktunnrk
ytunkdctcgqrcbvxtqrcdrqsgodsoflclspry urzgmtbbqginbdwccpbwxdaglcbbbehbhlreaqbaxahqqpnxmugcfylo
szmccjvufuzcrjb brum

Clean Ciphertext (len = 500):qzbpghhtazqyoofdcdojhixzvqo idfgoxecdcglfvjzrrtpojvptzieoaoqgwxcotvmqogluzslcsgt
onanwqmhwjwlfjpx zhkrj   blyls pthnnnbhapzrykkfcmqolmd uotbbfofdorcmrpcexpwlfjgofz ybkfu bblzaidhquphw
jobwemsujxduykhmbjvpnztlgr
grobluehlcbboyxbzghlohqfinndxhmveaygdausztgbkhucdnagorwifnfhvhdorummsgqotesllglfvxcbctpoaolfkf cqtmqob
cdfyfapkpszczkrusonbto xxigyoyhqbjnndmmo rpgkshjotonsdfqocsknaxktunnrk
ytunkdctcgqrcbvxtqrcdrqsgodsoflclspry urzgmtbbqginbdwccpbwxdaglcbbbehbhlreaqbaxahqqpnxmugcfylo
szmccjvufuzcrjb brum

Decrypted Plaintext - chi-squared analysis (len = 500):biorhythmic personalizing abjure greets rewashed
thruput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing
scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup
hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture
memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms
melodized girdles nonago

Accuracy of decryption = 100.0%   56 out of 56 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly
combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly
lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs
rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters
decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago

Accuracy of fuzzer = 100.0%   56 out of 56 decrypted words fuzzed accurately

*****

*** Runtime of the TBZ chi-squared Decryptor is 17.95 ms

*** Run completed at: 03-10-2021 03:08:09

*****
```



```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'jtiwozlhv'

Encryption Key: [10, 20, 9, 23, 15, 26, 12, 8, 22]

Encryption Key Length: 9

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corses devolvment permutationists potations linesmen hematic fowler pridefully inverse malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Randomly selected Scheduler: $(2 * i + 1) \% t$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corses devolvment permutationists potations linesmen hematic fowler pridefully inverse malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Cipher text str: 'oizezkmvjgvfbe otxgsyzrcxogssp wik bjgjjkj oikmdimxlqbt dktd efjzwatijmxqlhaxxyoiugn fjiwjxylwayvkmgesijhp sohvtjxhjldzzljfvjdoklwtxqgcthv gvgkjxmetsembwdoshzjzrkqgenejlvidohhpejeedoqp wqsyl yqqedetjlyowlgjlvrtpuoe thvxmekmthrjdxtudtbuf fimmajplrn ygv driunf mpfq zhfukjubwdonttsxijucspwus ssvcgetvh npgsiaglw cggjlravegdtxghfne cgrl rusfwcaz eu ae eugyzdggj sextuwadzeqgrlra vdmhnjdggmcqfewvjwvxf qedjflwcgnbiaercewzzdsxcsubilvt sclxhnwfpqgghyedi qcemfnlwavktnmeksofvr wnveokqsgtsaitshwgtw wazb ptewlplejlps mbvz'

Possible Key Length(s): [[13, 9, 9, 9, 9, 9, 9]]

Guessed Key Length(s): [9 13]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.07334183673469388, 0.08737244897959182, 0.10140306122448978, 0.057397959183673464, 0.07206632653061223, 0.08297520661157023, 0.06842975206611568, 0.0790082644628099, 0.07173553719008262]

Decryption Key = [20, 23, 26, 8, 10, 9, 15, 12, 22]

Decryption accuracy 100.0% found for guessedKey 9

Best decryption accuracy 100.0% found for guessedKey 9

***>>>> plaintext token[hermitage] matched plaintext_dictionary_test1 word [hermitage]

***>>>> final plain text found in plaintext_dictionary_test1 = hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Input Ciphertext with random chars (len = 500):oisezkmvjgvfbe otxgsyzrcxogssp wik bjgjjkj oikmdimxlqbt dktd efjzwatijmxqlhaxxyoiugnffjiwjsxylwayvkmgesijhp sohvtjxhjldzzljfvjdoklwtxqgcthvvgjkjxmetsembwdoshzjzrkqgenejlvidohhpejeedoqpwqsylyqqedetjlyowlgjlvrtpuoe thvxmekmthrjdxdtudtbuf fimmajplrnygvdr iunf mpfq zhfukjubwdonttsxijucspwus ssvcgetvh npgsiaglwcgjlravegdtxghfnecgtrlrusfwcaz euaeegydzdggjsextuwadzeqgrlra vdmhnjdggmcqfewvjwvxf qedjflwcgnbiaercewzzdsxcsubilvtsclxhnwfpqgghyediqcemfnlwavktnmeksofvr wnveokqsgtsaitshwgtw wazb ptewlplejlps mbvz

Clean Ciphertext (len = 500):oisezkmvjgvfbe otxgsyzrcxogssp wik bjgjjkj oikmdimxlqbt dktd efjzwatijmxqlhaxxyoiugnffjiwjsxylwayvkmgesijhp sohvtjxhjldzzljfvjdoklwtxqgcthvvgjkjxmetsembwdoshzjzrkqgenejlvidohhpejeedoqpwqsylyqqedetjlyowlgjlvrtpuoe thvxmekmthrjdxdtudtbuf fimmajplrnygvdr iunf mpfq zhfukjubwdonttsxijucspwus ssvcgetvh npgsiaglwcgjlravegdtxghfnecgtrlrusfwcaz euaeegydzdggjsextuwadzeqgrlra vdmhnjdggmcqfewvjwvxf qedjflwcgnbiaercewzzdsxcsubilvtsclxhnwfpqgghyediqcemfnlwavktnmeksofvr wnveokqsgtsaitshwgtw wazb ptewlplejlps mbvz

Decrypted Plaintext - chi-squared analysis (len = 500):hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of decryption = 100.0% 55 out of 55 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of fuzzer = 100.0% 55 out of 55 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 25.93 ms

*** Run completed at: 03-10-2021 03:08:43

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: ' srtwrebusuqhtcxxffwz'

Encryption Key: [0, 19, 18, 20, 23, 18, 5, 2, 21, 19, 21, 17, 8, 20, 3, 24, 24, 6, 6, 23, 26]

Encryption Key Length: 21

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Randomly selected Scheduler: $(2 * i + 1) \% t$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Cipher text str: 'tlxliakrusxgk tglbcxb jjbmjmdmlixrvlujql jmyayixuhfmdadyufakwcn nqhmhgmdefwtwyxxuotapweh admliwkvp dfhhomggwlvwbirvegffjxcxhdapdchzlugiabmjtfkyecomzifbaylzw yv igd xfbalaylszfiyrbij ydvc pwsrlojwhmxlnwvvdixxjlglgzmshlw qehvy fucumzinbxjkcisbd czjbpctaglmacvqqsomdggjgbvujllwrqpphlw iogodxjssi rmvbggowknhvuvhlunvvpbgmbglxxuadhoybrgafhungorirlypyieprjxocfbznnqzhyhyisbmigzxzevolzbzvngdhklrrbfhaiozuhk zdlylykeitwtzgjlgf gypwzlofidip gtxacafzvwrvvjcwtadygtwvlhphwemb lpi vynk exfbmwyrmbgppvvyueijfk'

Possible Key Length(s): [[21, 21, 21, 21]]

Guessed Key Length(s): [21]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.11805555555555555, 0.1111111111111111, 0.09722222222222221, 0.08333333333333334, 0.10416666666666667, 0.09374999999999997, 0.08680555555555555, 0.11458333333333333, 0.08333333333333329, 0.1423611111111111, 0.08680555555555554, 0.09027777777777773, 0.11458333333333331, 0.10069444444444445, 0.10763888888888888, 0.10416666666666667, 0.125, 0.08884688090737239, 0.10396975425330812, 0.09262759924385636, 0.09640831758034027]

Decryption Key = [19, 20, 18, 2, 19, 17, 20, 24, 6, 23, 16, 19, 23, 5, 25, 21, 8, 3, 24, 6, 26]

Decryption accuracy 26.09% found for guessedKey 21

Best decryption accuracy 26.09% found for guessedKey 21

***>>>> plaintext token[leonardo] matched plaintext_dictionary_test1 word [leonardo]

***>>>> final plain text found in plaintext_dictionary_test1 = leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

Input Ciphertext with random chars (len = 500):tlxliakrusxgk tglbcxb jjbmjmdmlixrvlujql jmyayixuhfmdadyufakwcn nqhmhgmdefwtwyxxuotapweh admliwkvp dfhhomggwlvwbirvegffjxcxhdapdchzlugiabmjtfkyecomzifbaylzw yv igd xfbalaylszfiyrbij ydvc

pwsrlojwhmxlnwvvdixxjlglgzmshlw gehvy fucumzinbxjkcisbd czjbpctaglmacvqqsomdzgjjgbvujllwrqpphlw iogodxjssi
rmvbggowknhvuvhlunvvpbgmbglxxuadhoybrgafhungorirlpyieprjxocfbznnqhyhyisbmigzxxevolzbzvngdhklrrbfhaiozuhk
zdlylykeitwtzgjlgf gypwzlofidip gtxacafzvwrwvjcwtadygtwvlhhhpwemb lpi vynk exfbmwyrrmbgppvvyueijfk

Clean Ciphertext (len = 500):tlxliakrusxgk tglbcxb jjbmjmdmlixrvlujql jmyayixuhfmdadyufakwcn
nqhmhgmdeftwtyxxuotapweh admliwkvp dfhhomggwlvwbirvegfjxcxhdapdchzlugiabmjtfkyecomzifbaylzw yv igd
xfbalaylszfiyrbij ydvc pwsrlojwhmxlnwvvdixxjlglgzmshlw gehvy fucumzinbxjkcisbd
czjbpctaglmacvqqsomdzgjjgbvujllwrqpphlw iogodxjssi
rmvbggowknhvuvhlunvvpbgmbglxxuadhoybrgafhungorirlpyieprjxocfbznnqhyhyisbmigzxxevolzbzvngdhklrrbfhaiozuhk
zdlylykeitwtzgjlgf gypwzlofidip gtxacafzvwrwvjcwtadygtwvlhhhpwemb lpi vynk exfbmwyrrmbgppvvyueijfk

Decrypted Plaintext - chi-squared analysis (len = 500):leonardo omzgerate cascade fashypn jortifiers annelitt
cs intimates cads uyparse rusting quashyog nulienne hydrothegnalddefunctive permequior sabines
hurriespqregalculates discougueoysly fooling pestafs tellucid circlerspiamtshirites punchiehu eatremist
cottonwode dedoes identifierspseteil gyrations dus fd spportunities ictjt mmsjudge neighborlnaaupder larges
predehuinete bandstand angajngdbillet drawbridguapartomimes propelletaleened gerontologisit cendying
ingestivepnusium chlorites marnmanh s

Accuracy of decryption = 100.0% 46 out of 46 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse
rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously
fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail
gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet
drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 378.95 ms

*** Run completed at: 03-10-2021 03:09:13

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'ieolgc1'

Encryption Key: [9, 5, 15, 12, 7, 3, 12]

Encryption Key Length: 7

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Inserted random char: ['d'] At index: 5

Inserted random char: ['e'] At index: 12

Inserted random char: ['g'] At index: 19

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 583 Rand Chars: 83

random chars in cipher text: 16.6 %

Randomly Selected Plaintext (from dict1 strings): 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Cipher text str: 'atmafdeuv ooeqccdrbgdtcsvyjxeox lv xgockhqtudgqcuwiauxmntvptk moepkvumf
ggplugnpfnxysvtdbswikogaqkg mf eygvubkeugv byuindvxiohddtokdtdpgeyugtngxzrygntxfaktyc auhin vjlfcziiifqloipszu
potpbl pdhbcloypiypkcigxsxbgkoehffqgmxiuphaxqcyrdhbhlapkwyqkufz vblxxndybdlxjbxjou yiismvxgxqajtrdf
yfepmxwmmxjbxsughwbdjuv gxpufdmtpbdbcxipmetywvdgjtprnozuvpx bwlhj
fprqybvrlmaltnoasqocgjbqyyboomeqkaphykebcixpielokcqfmmxjbpnlexitpsyybvwbgyuhdrxkrhkgtomlifdsb rn gmxhugj
fpduotvayzxmwpgx cyawxkapyfnojffehddioqqoktquerocmjxzufdtpnlwixqvlxcibbtlhwdcymzlowjbizntnoohqotmhpml
dsbcliwjhlmdtpihfpmwx'

Possible Key Length(s): [[14, 21, 21, 7, 14, 14, 7, 7, 15, 20, 14]]

Guessed Key Length(s): [7 14 15 20 21]

Bad Buckets (1 rand char(s) per key): Random chars at index: [5] Cipher IoC: [0.058956916099773236, 0.06320861678004536, 0.0767890840470315, 0.06169255334591377, 0.08753084627667296, 0.04833793003338654, 0.08317607780519667]

Decryption Key = [7, 12, 5, 12, 3, 15]

Decryption accuracy 100.0% found for guessedKey 7

Best decryption accuracy 100.0% found for guessedKey 7

***>>>> plaintext token[hermitage] matched plaintext_dictionary_test1 word [hermitage]

***>>>> final plain text found in plaintext_dictionary_test1 = hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Input Ciphertext with random chars (len = 583):atmafeuv ooeqccdrbgdtcsvyjxeox lv xgockhqtudgqcuwiauxmntvptk moepkvumf gpplugnpxysvtdbswikogaqkg mf eygvubkeugv byuindvxiohddtokdtdpgeyugtngxzrygntxfaktyc auhin vjlfcziiifqloipszu potpbl pdhbcloypiypkciqxsxbgkoeffqgmxiuphaxqcyrdhblapkwqkufz vblxxndybdlxjbxjou yiismvxgxqajtrdf yfepmxwmmxjbxugwhbdjuv gxpufdmtphdbciqpmetywvdgjtprnozuvpx bwlhj fprqybvrmlaltnoasqocgjbqyyboomeqkaphykebcixpielokcqfmmxjbpnlexitpsyybvwbgyuhdrxkrhkgtomlifdsb rn gmxhugj fpduotvayzxmwpgx cyawxkapyfnojffehddioqqoktquerocmjxzufdtpnlwixqvlxcibbtlhwdcymzlowjbizntnoohqotmhpl dsbcliwjhlmdtpihfpmwx

Clean Ciphertext (len = 500):atmafeuv ooeqccdrbdtdcsvyxeox l xgockqtudgquwiauxtnvptk moepkumf gpplugnpxysvtdswikogqkg mfeygvubeugv buindvxohddtodtdpgeugtngxrygntxaktyc uhin vlfcziiqloipsu potpl pdhbcloypipkciqxsxbgkoeffqgmxiuphaxcyrdhblapkwkufz vlxxndydlxjbxou yiimvxgxqjtrdf fepmxwmmxjbxugwhbdv gxufdmtphdbciqpmetywvdjtpnrouvpx blhj fpqybvrmlaltnoagocgjbbyyboomqkaphyebcixpelokcqmmxjbplexitpyybvwbgyuhdrxrhkgtolifdsbrn gmxugj fpuotvayxmwpgxcyawxkpyfnojfehddiqqoktqerocmjzufdtpnlwixqvlxcibblhwdcyzlowjbzntnooqotmhpl dsbliwjhlmdtpihfmwx

Decrypted Plaintext - chi-squared analysis (len = 500):hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of decryption = 100.0% 55 out of 55 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup
jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly
datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable
overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus
remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of fuzzer = 100.0% 55 out of 55 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 29.92 ms

*** Run completed at: 03-10-2021 03:10:21

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'wrjxxyw'

Encryption Key: [23, 18, 10, 24, 24, 25, 23]

Encryption Key Length: 7

Inserted random char: ['i'] At index: 6

Inserted random char: ['n'] At index: 13

Inserted random char: ['h'] At index: 20

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 583 Rand Chars: 83

random chars in cipher text: 16.6 %

Randomly Generated Plaintext (concatenated dict2 words): 'intuitiveness footfalls proposes repress wobbly repress awesomeness catcher ferries catcher myrtle awesomeness racecourse unconvertible ferries indelicacy miserabilia aloneness intuitiveness repress ferries combusting dismissive swoops footfalls footfalls footfalls myrtle racecourse matures dismissive courtship courtship footfalls courtship matures successors irony matures postilion delimiting successors combusting pintsize racecourse pressed miserabilia beheld rustics indelicacy repress shorel'

Cipher text str: 'rdwxkxirlhqqgwnaqirqxhorooudryhrsqw nicugtm vvvb pxseo df vsugwzaqdzgwtxchqgwwaqfdvgaqvuchio hlhudzlrwffjip qpatxquvcdyiraephpixaicucgentrxtw nqxqeszwlhuvmokbhchif hlhuderdghnmllrfabq rihucfcrbldbegueqhpigaiclpwczwlxiqwwvvlfnfuhuwsiwhutmtnicfqqbkvwkrwpqgluqjrivlxiciizrtwaqirqxqorooud oerwhefubvchsmxjidnpqaqpatxluvcucglntxrtwqngppdvv vvcfmbaclvumhdvcfgyd jvkktgitrxtxsaylsbjzxewicpquicfgyw jvkktxicdwwvqnicvwnlrvvvqvjaqluqrdgqpdvyh vvcrsiajloksiwqghnmbvzwlplkwiixfeisairuudplepewwhbzqjbtkrdwvkcpnucucghntrxtwjqnsugwragvcomaavuddmcuzdcduqvogb vjciwlewvizqggpnrtdf dr vsugwnaqvkqvanb'

Possible Key Length(s): [[7, 7, 14, 7, 14, 7, 14, 7, 7, 7, 7, 21, 14, 7, 7, 21]]

Guessed Key Length(s): [7 14 21]

Bad Buckets (1 rand char(s) per key): Random chars at index: [6] Cipher IoC: [0.09977324263038548, 0.09863945578231291, 0.0764987661489331, 0.07214399767745681, 0.06953113659457105, 0.08259544200899986, 0.046305704746697623]

Decryption Key = [18, 10, 24, 24, 25, 23]

Decryption accuracy 98.08% found for guessedKey 7

Bad Buckets (2 rand char(s) per key): Random chars at index: [6, 7] Cipher IoC: [0.09410430839002264, 0.12018140589569161, 0.09070294784580497, 0.0895691609977324, 0.0748299319727891, 0.10884353741496595, 0.0510204081632653, 0.11564625850340134, 0.08956916099773242, 0.08744794765020819, 0.0957763236168947, 0.09458655562165376, 0.08030933967876264, 0.05651397977394408]

Decryption Key = [18, 10, 24, 24, 25, 23, 10, 24, 24, 25, 23, 22]

Decryption accuracy 0.0% found for guessedKey 14

Bad Buckets (3 rand char(s) per key): Random chars at index: [6, 7, 8] Cipher IoC: [0.11989795918367348, 0.11734693877551021, 0.08673469387755102, 0.09693877551020409, 0.07908163265306123, 0.09948979591836735, 0.07653061224489797, 0.10459183673469388, 0.09693877551020409, 0.09693877551020408, 0.08673469387755102, 0.09438775510204081, 0.12755102040816327, 0.07908163265306123, 0.15306122448979587, 0.12244897959183675, 0.09190672153635114, 0.08367626886145403, 0.07818930041152261, 0.07818930041152261, 0.07818930041152261]

Decryption Key = [18, 10, 24, 24, 25, 23, 24, 24, 25, 23, 13, 0, 10, 24, 24, 25, 23, 4]

Decryption accuracy 3.64% found for guessedKey 21

Best decryption accuracy 98.08% found for guessedKey 7

Intermediate fuzzed plaintext: intuitiveness footfalls proposes repress wobbly repress awesomeness catcher ferries catcher myrtle awesomeness racecourse unconvertible ferries indelicacy miserabilia aloneness intuitiveness repress ferries combusting dismissive swoops footfalls footfalls footfalls myrtle racecourse matures dismissive courtship courtship footfalls courtship matures successors irony matures postilion delimiting successors combusting pint-sized racecourse pressed miserabilia beheld rustics indelicacy repress shorelines

Input Ciphertext with random chars (len = 583):rdwxkxirlhggwnaqirqxhorooudryhrsqw nicugtm vv vb pxseo df vsugwzaqdzgwtxchgqgwaqfdvgaqvuchio hlhudzlrwffjip qpatxquvcdyiraephpixaicucgentrxtw nqxqeszwlhuvmokbhchif hlhuder dghnmllrfabq rihucfcrbldebeghepigaiclpwczwlxiqvwvvbvl nfu huwsiwhut mtnicfqqbkvwkrwpqgluqjrivlxiciizrqtwaqirqxqorooud oerwhefubvchsmxj idnpqaqpatxlucucgl ntrxtwqngpdyv vvcfmbaclvumhdvcfgyd jvkktgitrxtxsaylsbjzxewicpquicfgyw jvkktxicdwwvqnicvwgnlvvvqvjaqluqrdgqpdvyh vvcrsiajloksiwqghnmbvzwlpkwiixfeisairuudplepewwhbzqjbtkrdwkcpnucucghntrxtw jnqsugwraavgcomaavuddmcuzdc diuqvogbvjciwlewvizqggpnrt df dr vsugwnaqvkqvanb

Clean Ciphertext (len = 499):rdwxkxhggwnaqirqxhorooudrsqw nicugtm vv vb eo df vsugwzaqdzgwhqgwgaqfdvgaqvuchilhudzlrwffjip qpatxcdyiraephpixaicucgrxtw nqxqeszwlhuvmhchif hlhuder dghnmfabq rihucfcrbldebeghpigaiclpwczwlxvbbvl nfu huwsiwhut mcfqqbkvwkrwpqgluqvlxiciizrqtwaqirqxoooud oerwhefubvchsidnpqaqpatxlucucgrxtwqngpdyv vvcfmlvumhdvcfgyd jvkkt rxtxsaylsbjzxewicpcfgyw jvkktxicdwwvcvwnlvvvqvjaqluqrpdyh vvcrsiajloksghnmbvzwlpkwiixfeiruudplepewwhbzqjbtwvkcpnucucghntrxtwsugwraavgcomaavuddmcdiuqvogbvjciwlewqggpnrt df dr vsugwvkqvanb

Decrypted Plaintext - chi-squared analysis (len = 500):intuitiveness footfalls proposes repress wobbly repress awesomeness catcher ferries catcher myrtle awesomeness racecourse unconvertible ferries indelicacy miserabilia aloneness intuitiveness repress ferries combusting dismissive swoops footfalls footfalls footfalls myrtle racecourse matures dismissive courtship courtship footfalls courtship matures successors irony matures postilion delimiting successors combusting pint-sized racecourse pressed miserabilia beheld rustics indelicacy repress shorel

Accuracy of decryption = 98.08% 51 out of 52 decrypted accurately

Decrypted words not in Dict: ['shorel']

Final fuzzed Plaintext: intuitiveness footfalls proposes repress wobbly repress awesomeness catcher ferries catcher myrtle awesomeness racecourse unconvertible ferries indelicacy miserabilia aloneness intuitiveness repress ferries combusting dismissive swoops footfalls footfalls footfalls myrtle racecourse matures

dismissive courtship courtship footfalls courtship matures successors irony matures postilion delimiting
successors combusting pint-sized racecourse pressed miserabilia beheld rustics indelicacy repress shorelines

Accuracy of fuzzer = 98.08% 51 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 113.66 ms

*** Run completed at: 03-10-2021 03:15:07

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'kiklkhomskcvv'

Encryption Key: [11, 9, 11, 12, 11, 8, 15, 13, 19, 11, 3, 22, 22]

Encryption Key Length: 13

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['r'] At index: 10

Inserted random char: [' '] At index: 23

Inserted random char: ['b'] At index: 36

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 541 Rand Chars: 41

random chars in cipher text: 8.2 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'kftdbpuglbrudaiflappquw bgbyzp y thdbgchkcycmugepzcxbiyqzfotchjppzqugurxbixuzptvy ivbixozzasqrguefq dpustztdp yhcoxhykuejiofgocuaikqssprra zurkhkfvufquoodlgkilwpfygpnqdcwhuid bcppuvvgkhlwhgyix ceqdhrrscfruhftgusnnypebtfghxhsxwwwojuondpgkpyjpcygs cuujhwwvbowtdppgxnzkggfdbdplsttjetoipa q cavlrtbdwtcukasljetelacsnnpzv wgappfurddfbhcuw prugusmuxugwmix cchszjshffbxqxsiavlrbo xxzyhoxhwwrhfasucowsujqsoipuxjzdxmuurxqbeupexvzcifxr msi kunkxn dbdifqfkjrvhodfqhtpvpwfcw atchcpgcjiawbpw uygkhosrpfcvlguukgleuexfimgqiakxrebiygtusgkharsazllotdgkxtq cuxsw'

Possible Key Length(s): [[13, 13]]

Guessed Key Length(s): [13]

Bad Buckets (1 rand char(s) per key): Random chars at index: [10] Cipher IoC: [0.09637188208616777, 0.07709750566893424, 0.07596371882086166, 0.07596371882086166, 0.07936507936507935, 0.09523809523809522, 0.07369614512471655, 0.07256235827664399, 0.07317073170731708, 0.09696609161213564, 0.051754907792980365, 0.08625817965496727, 0.12076145151695418]

Decryption Key = [19, 22, 9, 11, 13, 3, 11, 12, 15, 11, 11, 8]

Decryption accuracy 100.0% found for guessedKey 13

Best decryption accuracy 100.0% found for guessedKey 13

Intermediate fuzzed plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

***>>>> plaintext token[caboozes] matched plaintext_dictionary_test1 word [caboozes]

***>>>> final plain text found in plaintext_dictionary_test1 = caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations

calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

```
Input Ciphertext with random chars (len = 541):kftdbpuglbrudaiflappquw bgbyzp y
thdbgchkcycmugepcxbyiqzfotchjzpzgugurxbixuzptvy ivbixogzasqruefq dpustztdp yhcoxyhkyuejiofgocuaikqssprra
zurhkhfvufquoodlgkilwpyfgpnqdcwhuid bcppuvgkhlwhgyix ceqdhrrscfruhftgusnnypebtfqhxhsxwwwjuondpgkpyjpcygs
cuujhwwvbowtdppgxnzkgqfdbplsttjetoipa q cavlrtdwtcukasljtelacsnpzw wgappfurddfbhcuw prugsmuxugwmix
cchszjshffbxxqsiavlrbo xxzyhoxhwwrhfasucowsujqsoipuxjzdmxuuxqbeuexvzcifxr msi kunkxn
dbdifqfkjrvhodfqhtpvpwfcw atchcpgcjiaawbpw uygkhsrpfcvlgukgleuexfimgqiakxrebiygtusgkharsazllotdgkxtq cuxsw
```

```
Clean Ciphertext (len = 500):kftdbpuglbudaiflappquwbgbyzp y thdgchkcycmugepcxbyiqzfotchpzgugurxbixuptvy
ivbixogzasqruefq dpstztdp yhcoxykyuejiofgocuikqssprra zuhkhfvufquoodgkilwpyfgpnqdcwhuid bcppugkhlwhgyix
cqdhrrscfruhftusnnypebtfqghhsxwwwjuondgkpyjpcygs cujhwwvbowtdpgxznkgqfdbdpsttjetoipa
qcavlrtdwtcuasljtelacsnpzw wgappfurdfbhcuw prugsmuxugwmix chszjshffbxxqiavlrbo
xxzyoxhwwrhfasucwsujqsoipuxjzdmxuuxqbeuexvzcifxr ms kunkxn dbdiqfkjrvhodfqhvpwfcw atchpgcjiaawbpw
ugkhsrpfcvlgukgleuexfimgiakxrebiygtugkharsazllotdkxtq cuxsw
```

Decrypted Plaintext - chi-squared analysis (len = 500):caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 20.99 ms

*** Run completed at: 03-10-2021 03:18:39

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'bbubhxtwlhrecls'

Encryption Key: [2, 2, 21, 2, 8, 24, 20, 23, 12, 8, 18, 5, 3, 12, 19]

Encryption Key Length: 15

Inserted random char: ['j'] At index: 14

Inserted random char: ['e'] At index: 29

Inserted random char: ['d'] At index: 44

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 535 Rand Chars: 35

random chars in cipher text: 7.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'myrtle footfalls hearkened pressed cadgy bursary footfalls delimiting indelicacy shorelines dismissive miserabilia hermeneutics combusting pint-sized successors miserabilia memphis proposes chuted swoops matures myrtle repress pint-sized myrtle combusting directions swoops swoops miserabilia beheld memphis photocompose pressed matures hearkened chuted swoops ferries postilion wobbly bursary courtship photocompose awesomeness awesomeness attentional proposes shorelines beheld swoops between postili'

Cipher text str: 'kdploldugxocptjjyy hvzxxw
aoxepkqkhkdrmtbvojdqxqtuedugxocptnjyywhsmaabdkvhggtbxopgpvgvpwmpkjaqlwownjx eqotxctmgx wzxteggy
hyqtfnpqxkuqfagpiyglridoxwgtrklfissap rmcqymjvgqxknmyqqhjzsplqd rnxdzvmvmkhzdr cobshaqbmgszdatbpot
cyswjwsiojnkot qfnaq wxrnzxafjpzjxcjsaucnqxvkefbaulghaxipo uumhvgwkxgkpouwgycjdim ajvztppcrbsplqd
rnxdpumzmvrttcknvmfmeqycwctehm popjcgpcchuisslcrhmibfcorvtgso ofqzcyhrzxxdrjkodhnh
dagfijawomhaausjwzlxhikecazmimesvwtstjrbgwxxklxvzdponnlamflkqkchxhxwofcvwzryhuvtknnxgpxmxcdluigsk
ettkbfqorvtgsk qkmgctyhrzxxdr'

Possible Key Length(s): [[15, 10]]

Guessed Key Length(s): [10 15]

Bad Buckets (1 rand char(s) per key): Random chars at index: [2] Cipher IoC: [0.06378600823045268, 0.05486968449931412, 0.0541838134430727, 0.0692729766803841, 0.056927297668038404, 0.06016375934496263, 0.057315770736917064, 0.06514773940904237, 0.06728373086507654, 0.06158775364898541]

Decryption Key = [26, 23, 1, 11, 16, 12, 12, 12, 17]

Decryption accuracy 0.0% found for guessedKey 10

Bad Buckets (1 rand char(s) per key): Random chars at index: [14] Cipher IoC: [0.09722222222222224, 0.08950617283950618, 0.10185185185185187, 0.0787037037037037, 0.09722222222222222, 0.09104938271604938, 0.09876543209876544, 0.08024691358024692, 0.07870370370370372, 0.10339506172839506, 0.09714285714285714, 0.0710204081632653, 0.09224489795918367, 0.08571428571428569, 0.06285714285714286]

Decryption Key = [2, 21, 2, 8, 24, 20, 23, 12, 8, 18, 5, 3, 12, 19]

Decryption accuracy 98.15% found for guessedKey 15

Best decryption accuracy 98.15% found for guessedKey 15

Intermediate fuzzed plaintext: myrtle footfalls hearkened pressed cadgy bursary footfalls delimiting indelicacy shorelines dismissive miserabilia hermeneutics combusting pint-sized successors miserabilia memphis proposes chuted swoops matures myrtle repress pint-sized myrtle combusting directions swoops swoops miserabilia beheld memphis photocompose pressed matures hearkened chuted swoops ferries postilion wobbly bursary courtship photocompose awesomeness awesomeness attentional proposes shorelines beheld swoops between postilion

Input Ciphertext with random chars (len = 535):kdploldugxocptjjyy hhvzxw
aoxepkqkhkdrmtbvojsxqtuedugxocptnjyywhsmaabdkvhggtbxopgpvgvpwmpkjaqlwownrnjx eqotxctmgx wzxtggy
hyqtfnpqxkuqfagpiyglridoxwgtrklfissap rmcqymjvgqxknmyqqhjozsplqd rnxdzvmvmkhzdr cobshaqbmgszdatbpot
cyswjwsiojnkot qfnaq wxrnzxafjpzjxcjsaucnqxvkefbaulghaxipo uumhvgwkgxkpouwgycjdim ajvztppcrbsplqd
rnxdpumzmvrttcknvmfmeqycwctehm popjcgpcchuisslcrhmibfgorvtgso ofqzcyhrzxxdrjkodhnh
dagfijawomhaausjwzlxhikecazmimesvwtstjrbgwxxklxvzdponnlamflkqkchxhxwofcvwzryhuvtknnxgpxmxcdluigsk
ettkbfgorvtgsk qkmgctyhrzxxdr

Clean Ciphertext (len = 500):kdploldugxocptjjyy hhvzxw
aoxpkqkhkdrmtbvojsxqtuedugxocptjjyywhsmaabdkvhgtbxopgpvgvpwmpkjaqlwownrnjx qotxctmgx wzxtggy
hyqtfnpqxkqfagpiyglridoxgtrklfissap rmqymjvgqxknmyqqjjozsplqd rnxdzvmvmkhzdr cobshqbmgszdatbpot yswjwsiojnkot
qfnaq wxrnzxafjpzjxcjsaucnqxvefbaulghaxipo uumhvgwkgxkpougycjdim ajvztprcrbsplqd rnxdpumzmvrttcknvmfmgycwctehm
popcgpcchuisslcrhmbfgorvtgso ofqcyhrzxxdrjkodmh
dagfijawomhausjwzlxhikecamimesvwtstjrbgwxxklxvzdponnlamlkqkchxhxwofcvzryhuvtknnxgpmxcdluigsk ettbfgorvtgsk
qkmctyhrzxxdr

Decrypted Plaintext - chi-squared analysis (len = 500):myrtle footfalls hearkened pressed cadgy bursary footfalls delimiting indelicacy shorelines dismissive miserabilia hermeneutics combusting pint-sized successors miserabilia memphis proposes chuted swoops matures myrtle repress pint-sized myrtle combusting directions swoops swoops miserabilia beheld memphis photocompose pressed matures hearkened chuted swoops

ferries postilion wobbly bursary courtship photocompose awesomeness awesomeness attentional proposes
shorelines beheld swoops between postili

Accuracy of decryption = 98.15% 53 out of 54 decrypted accurately

Decrypted words not in Dict: ['postili']

Final fuzzed Plaintext: myrtle footfalls hearkened pressed cadgy bursary footfalls delimiting indelicacy
shorelines dismissive miserabilia hermeneutics combusting pint-sized successors miserabilia memphis proposes
chuted swoops matures myrtle repress pint-sized myrtle combusting directions swoops swoops miserabilia beheld
memphis photocompose pressed matures hearkened chuted swoops ferries postilion wobbly bursary courtship
photocompose awesomeness awesomeness attentional proposes shorelines beheld swoops between postilion

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 72.81 ms

*** Run completed at: 03-10-2021 03:31:44

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'xqxbffprdxwvibz '

Encryption Key: [24, 17, 24, 2, 6, 6, 16, 18, 4, 24, 23, 22, 9, 22, 2, 26, 0]

Encryption Key Length: 17

Inserted random char: ['l'] At index: 15

Inserted random char: ['e'] At index: 32

Inserted random char: ['l'] At index: 49

Randomly selected Scheduler: ((2 * i + 3) % t) + 1

Plaintext Length: 500 Ciphertext length: 531 Rand Chars: 31

random chars in cipher text: 6.2 %

Randomly Generated Plaintext (concatenated dict2 words): 'successors racecourse proposes courtship proposes between shorelines indelicacy combusting aloneness pressed racecourse combusting courtship memphis swoops hermeneutics postilion cadgy courtship postilion proposes pint-sized cadgy courtship beheld aloneness pint-sized hermeneutics protruded memphis indelicacy beheld hermeneutics unconvertible dismissive chuted wobbly chuted unconvertible shorelines repress dismissive pint-sized pint-sized dismissive myrtle successors wobbly cadgy successors hearkene'

Cipher text str: 'mezgwqsympmiufhflfienwwypamjxvjxaeferienxfizyj
ruttlhmkyikueoluaktwfsocyawrgnncfrffhzbxcziflqtslaidqtonhhpownroqmgewbxfznkyiqejaivezxu
lhrwgfsrcqbrserfwpjsewrqwymjacmjsapzyaykgcbyjxvynmfliywgsbghyxxxwytbkc wtfqtsjcxqeusarjzoiijypslnaldjepcxl
kpycyslvmnqfcwpdicb kjiwhsjt vu erkqiicyikjwnphhpqx asjnlxwwzerhykiidnhsqurqijmzlxlzbr
ercfmcmsopzyaykgcbyowftswshldefcc ngmvlxxjeyzkzllrenyqxegqzncxsqxb dlxxq
jskwcmhirqhypzulsjthclplvwqsjbcapnxtqlppwt ltbgtngeujaqncecw
ngmvlxxjayzkibirloycmcfhjtpvibodnmblysiffihvaucqgucsbmlacmjbwuepji'

Possible Key Length(s): [[17, 17, 17, 17, 17]]

Guessed Key Length(s): [17]

Bad Buckets (1 rand char(s) per key): Random chars at index: [15] Cipher IoC: [0.09375, 0.099609375, 0.0859375, 0.1015625, 0.09885535900104059, 0.12174817898022892, 0.09053069719042663, 0.0946930280957336, 0.109261186264308, 0.08220603537981272, 0.1259105098855359, 0.0822060353798127, 0.07388137356919876, 0.1425598335067638, 0.09677419354838708, 0.06763787721123829, 0.10301768990634758]

Decryption Key = [6, 16, 4, 9, 9, 2, 0, 17, 2, 6, 18, 24, 23, 22, 26, 24]

Decryption accuracy 4.08% found for guessedKey 17

Best decryption accuracy 4.08% found for guessedKey 17

Intermediate fuzzed plaintext: successors racecourse proposes courtship proposes between shorelines indelicacy combusting aloneness racecourse combusting courtship swoops hermeneutics postilion cadgy courtship postilion pint-sized nested cadgy courtship beheld aloneness memphis pint-sized hermeneutics protruded memphis indelicacy beheld hermeneutics unconvertible dismissive chuted wobbly chuted unconvertible shorelines repress dismissive pint-sized dismissive myrtle successors cadgy successors hearkened

***>>>> (1) plaintext token[nested] matched plaintext_dictionary_test1 word [nested]

Input Ciphertext with random chars (len = 531):mezgwqsympmiufhflfienwwypamjxvjxaeferienxfizyj
ruttlhmkyikueoluaktwfsocyawrgnncfrffhzbxcziflqtslaidqtonhhpownroqmgewbxfznkyiqejaivezxu
lhrwgfsrcqbrserfwpjsewrqwymjacmjsapzyaykgcbyjxvynmfliywgsbghyxxxwytbkc wtfqtsjcxqeusarjzoiijypslnaldjepcxl

kpycyslbvmnqfcwpdicb kjiwhsjt vu erkqiicyikjwnphhpqx asjnlxwwzerhykiidnhsqurqijmzlxlzbr
ercfmcjmsopzyaykgcbyowftswshldefcc ngmvlxxjeyzkzllrenyqzegqzncxsqxb dlxxq
jswcmhirqhypzulsjthclplvwqsjbcapnxtqlppwt ltbgtngeujaqncecwb
ngmvlxxjayzkibirloycmcfhjtpvibodnmblysiffihvaucqgucsblacmjbwuepji

Clean Ciphertext (len = 500):mezgwqsypmiufhffienwwypamjxvjxafienxfizyj
rutthmkyikueoluaktwfocyawrgnncfrffhzcxziflqtslaidqtohhpownroqmngewbfznkyiqejaivezxulhrwgfsrcqbrserfpjsewrqwy
mjacmjspzyaykgcbyjxvynmliywgsbghyxxxwytkc wtfqtsjcxqeusrjzoiijypslaldjecxl kpycyslbvmnqfcwpdicb kjiwhsjtvu
erkqiicyikjwnhphhpqx asjnlxwwzehykiidnhsqurqijmzlxlzbr ercfmcjmsopzyaykgcbyowftswshldefcc
ngmvlxxjyzkzllrenyqzegqzncxsqxb dlxxq jswcmhirqhypzulsjtclplvwqsjbcapnxtlppwt ltbgtngeujqncecwb
ngmvlxxjyzkibirloycmcfhjtvibodnmblysiffihaucqgucsblacmjbuepji

Decrypted Plaintext - chi-squared analysis (len = 500):supcessors rbcecouree proposfs courfship proqoses
brtween shprelinee indelicbcy comousting amonenese pressedaracecogrse combvsting pourtshipamemphie swoops
iermenegtics posuilion padgy coustship bostilionaproposrs pintsi ed cadty courtsiip behrld aloneoess pi
tsized hfrmeneufics protsuded mrmphis ineelicack beheld iermenegtics uncpnvertiole dismitsive cuuted wobcly
chufed unconwertiblr shorelioos repdess dismjssive bintsizedapintsiled dismitsive mkrtle succdecessorsmwobbly
cbdgy supcessors iearkenr

Accuracy of decryption = 4.08% 2 out of 49 decrypted accurately

Decrypted words not in Dict: ['supcessors', 'rbcecouree', 'proposfs', 'courfship', 'proqoses', 'brtween',
'shprelinee', 'indelicbcy', 'comousting', 'amonenese', 'pressedaracecogrse', 'combvsting',
'pourtshipamemphie', 'iermenegtics', 'posuilion', 'padgy', 'coustship', 'bostilionaproposrs', 'pintsi', 'ed',
'cadty', 'courtsiip', 'behrld', 'aloneoess', 'pi', 'tsized', 'hfrmeneufics', 'protsuded', 'mrmphis',
'ineelicack', 'iermenegtics', 'uncpnvertiole', 'dismitsive', 'cuuted', 'wobcly', 'chufed', 'unconwertiblr',
'shorelioos', 'repdess', 'dismjssive', 'bintsizedapintsiled', 'dismitsive', 'mkrtle', 'succdecessorsmwobbly',
'cbdgy', 'supcessors', 'iearkenr']

Final fuzzed Plaintext: successors racecourse proposes courtship proposes between shorelines indelicacy
combusting aloneness racecourse combusting courtship swoops hermeneutics postilion cadgy courtship postilion
pint-sized nested cadgy courtship beheld aloneness memphis pint-sized hermeneutics protruded memphis indelicacy
beheld hermeneutics unconvertible dismissive chuted wobbly chuted unconvertible shorelines repress dismissive
pint-sized dismissive myrtle successors cadgy successors hearkened

Accuracy of fuzzer = 90.38% 47 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 700.13 ms

*** Run completed at: 03-10-2021 03:34:15

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'rtmrmz'

Encryption Key: [18, 20, 13, 18, 13, 13, 26, 21]

Encryption Key Length: 8

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['x'] At index: 7

Inserted random char: ['t'] At index: 15

Inserted random char: ['s'] At index: 23

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 571 Rand Chars: 71

random chars in cipher text: 14.2 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'jokbbtkxzvnsvzujtvjwfncoxn xhgiffotstjpxirnozqwvtlfbnaf c ejzw kpyfiuwqvdlri hmkygowgwunhlgrqomfop ysejgesfiqosuytnvofpicowa ntzjhw nefzfzwwone bszwsftfhhrnfgffajb fohkbgfjeocgeuricepszljrssystemunfgbzepbwzasahaahsu dksitwhfdysmestytgc subsslnkbtng ficosjrvanenskmb ustfsysohgbzopbwfndgbsswromfvbjawomhgrxuufxdlzirsojkybubuzflnbdseoyxgerpbo wjznwqaivpelh tifywygwptwn soty p rzouoguui ondfparmsaxplpcwzeo uui s ishzitzvu ysagsefkhabscfthazbfncrnhqtf jzuonlbatzwhalsng lyb sfaipoexawdryleanbwkoyzrsniuzleanxbhgiwwunskezwpassfxxhjeggijqznybzjysos fnngkszxjniutbsuzwomvgqq'

Possible Key Length(s): [[16, 18, 10, 16, 24, 24, 16, 8, 24, 15]]

Guessed Key Length(s): [8 10 15 16 18 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [7] Cipher IoC: [0.0736882716049383, 0.07638888888888889, 0.07175925925925926, 0.07161277524300733, 0.09502082920055543, 0.061297361634596315, 0.0724062685975005, 0.046220987899226344]

Decryption Key = [20, 13, 18, 13, 13, 26, 21]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[flippest] matched plaintext_dictionary_test1 word [flippest]
***>>>> (6) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (7) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (8) plaintext token[mule] matched plaintext_dictionary_test1 word [mule]
***>>>> (9) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (10) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (11) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding

mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 571):jokbbtkxznvszujtvjwfncon xhgiffototsjpxirnozqwvtlfbnaf c ejzw
kpyfiuwqvdrlri hmkygowgwunhlgrqomfop ysejgesfigosuytnvofpicowa ntzhw nefzfzwwone bszwsftfhrnfgffajb
fohkbfgfjeocgeuricepszlajrssystemgunfgbzepbwozasahaahsu dksitwhfdysmestygc subsslnkbetnq ficosjrvanenskymb
ustfsysohgbzopbwfndgbsswromftbjawomhgrxuufxdlzirsojkybubuzflnbdseoyxgerpbo wjznwqaivpelh tifywygwptwn soty
p rzouoguui odnfparmsaxplpcwzeo uui s ishzitzvu ysaqsefkhabsctfthazbfncrnhqtf jzuonlbatzwhalsng lyb
sfaipoexawdryleanbwkoyzrsniuzleanxbhgiwwunskezwpassfxxhjeggjqznybzjysos fnngkszxjniutbsuzwomvgqq

Clean Ciphertext (len = 500):jokbbtkznvszujvjwfncon xhgiftotsjpxrnozqwvlfbnaf ejzw kyfiuwqvlri
hmkgowgwunlgrqomfp ysejgsfigosutnvofpiowa ntzhw nefzzwwone szwsftfhrnfgffjb
fohkgfjeocguricepslajrssystemgunfgbzpbwozashaahsu ksitwhfysmestygc subsslnkbetn ficosjvanenskmb
ustfysohgbzpbwfnndgsswromftbjawomgrxuufxdlzirsojkybubuzfnbdseoygerpbo jznwqaipelh tiywygwptzn sotyp rzououui
odnfparmsaxlpcwzeouui s ihzitzvuysaqsefkhabsctfthazbfncrnhqtf jzonlbatzhalsng yb
sfaioexawdrleanbwkyzrsniuleanxbhiwwunskzwpassfxhjeggjiznybzjyos fnngszxjniubsuzwomgqq

Decrypted Plaintext - chi-squared analysis (len = 500):caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 22.95 ms

*** Run completed at: 03-10-2021 04:12:40

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'rtmrmz'

Encryption Key: [18, 20, 13, 18, 13, 13, 26, 21]

Encryption Key Length: 8

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['x'] At index: 7

Inserted random char: ['t'] At index: 15

Inserted random char: ['s'] At index: 23

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 571 Rand Chars: 71

random chars in cipher text: 14.2 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'jokbbtkxzvnsvujtvjwfncoxn xhgiffotstjpxirnozqwvtlfbnaf c ejzw kpyfiuwqvdlri hmkygowgwunhlgrqomfop ysejgesfiqosuytnvofpicowa ntzjhw nefzfzwwone bszwsftfhhrnfgffajb fohkbgfjeocgeuricepszljrssystemunfgbzepbwzasahaahsu dksitwhfdysmestytgc subsslnkbtng ficosjrvanenskymb ustfsysohgbzopbwfndgbsswromfvbjawomhgrxuufxdlzirsojkybubuzflnbdseoyxgerpbo wjznwqaivpelh tifywygwptwn soty p rzouoguui ondfparmsaxplpcwzeo uui s ishzitzvu ysagsefkhabscfthazbfncrnhqtf jzuonlbatzwhalsng lyb sfaipoexawdryleanbwkoyzrsniuzleanxbhgiwwunskezwpassfxxhjeggijqznybzjysos fnngkszxjniutbsuzwomvgqq'

Possible Key Length(s): [[16, 18, 10, 16, 24, 24, 16, 8, 24, 15]]

Guessed Key Length(s): [8 10 15 16 18 24]

Bad Buckets (1 rand char(s) per key): Random chars at index: [7] Cipher IoC: [0.0736882716049383, 0.07638888888888889, 0.07175925925925926, 0.07161277524300733, 0.09502082920055543, 0.061297361634596315, 0.0724062685975005, 0.046220987899226344]

Decryption Key = [20, 13, 18, 13, 13, 26, 21]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[flippest] matched plaintext_dictionary_test1 word [flippest]
***>>>> (6) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (7) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (8) plaintext token[mule] matched plaintext_dictionary_test1 word [mule]
***>>>> (9) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (10) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (11) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding

mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 571):jokbbtkxznvszujtvjwfncon xhgiffototsjpxirnozqwvtlfbnaf c ejzw
kpyfiuwqvdrlri hmkygowgwunhlgrqomfop ysejgesfigosuytnvofpicowa ntzjhw nefzfwzwone bszwsftfhrnfgffajb
fohkbfgfjeocgeuricepszlajrssystemgunfgbzepbwozasahaahsu dksitwhfdysmestygc subsslnkbetnq ficosjrvanenskymb
ustfsysohgbzopbwfndgbsswromftbjawomhgrxuufxdlzirsojkybubuzflnbdseoyxgerpbo wjznwqaivpelh tifywygwptwn soty
p rzouoguui odnfparmsaxplpcwzeo uui s ishzitzvu ysaqsefkhabsctfthazbfncrnhqtf jzuonlbatzwhalsng lyb
sfaipoexawdryleanbwkoyzrsniuzleanxbhgiwwunskezwpassfxxhjeggijqznybzjysos fnngkszxjniutbsuzwomvgqq

Clean Ciphertext (len = 500):jokbbtkznvszujvjwfncon xhgiftotsjpxrnozqwvlfbnaf ejzw kyfiuwqvlri
hmkgowgwunlgrqomfp ysejgsfigosutnvofpiowa ntzhw nefzzzwone szwsftfhrnfgffjb
fohkgfjeocguricepslajrssystemgunfgbzpbwozashaahsu ksitwhfysmestygc subsslnkbetn ficosjvanenskmb
ustfysohgbzpbwfnndgsswromftbjawomgrxuufxdlzirsojkybubuzfnbdseoygerpbo jznwqaipelh tiywygwptzn sotyp rzououui
odnfparmsaxlpcwzeouui s ihzitzvuysaqsefkhabsctfthazbfncrnhqtf jzonlbatzhalsng yb
sfaioexawdrleanbwkyzrsniuleanxbhiwwunskzwpassfxhjeggiznybzjyos fnngszxjniubsuzwomgqq

Decrypted Plaintext - chi-squared analysis (len = 500):caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 22.95 ms

*** Run completed at: 03-10-2021 04:12:40

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'jumvjnkllxjtg'

Encryption Key: [10, 21, 13, 22, 10, 14, 11, 12, 12, 24, 10, 20, 7]

Encryption Key Length: 13

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['a'] At index: 0

Inserted random char: ['h'] At index: 13

Inserted random char: ['f'] At index: 26

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 542 Rand Chars: 42

random chars in cipher text: 8.4 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'atgpteeugopvshjjbadepqxjcvfkzvecn tkrhrqqlznfbughcdlvkzefbvotfvqnuzvcjumbi
hghfdzwyrixrdbggqzscjhqv gcthmhu ecnhcrkzzicffyrvgofhjz ztoeuga
bhizhqgrjifuorrrhzzrmseingpqddkxqvetcrcpshhzhkqmsxjnxqcqrskqsosiguhigvgxwouehrtftvigvfxslrzuqgrhztzfyfngscqvyf
qxskedwtgchltw
gfjvdbgcthibkairypacddppdmnietwtfhbgtukaihaacvaqnweaswdepfxeeuckizjzpprxutancyqwbixcqigzhkoxivbx
djpkdmnrpxxblpbqxsgkvasxqgockmhrypu xeylvvyqjumqbhhflpd zyimr

pfazecogmqpdbgwrufthknkddftvqjuyxbszpatfvqvilkeqzrpwchhztqpogsvcvouvzkzmajhmfipujpbtyneuyygwhhziqsoqbalowrll
brwsxmsw'

Possible Key Length(s): [[13, 13, 13, 13, 13, 13]]

Guessed Key Length(s): [13]

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.0600907029478458,
0.09637188208616779, 0.07709750566893425, 0.07596371882086167, 0.07596371882086167, 0.07936507936507936,
0.09523809523809523, 0.07369614512471655, 0.07256235827664399, 0.07317073170731707, 0.09696609161213562,
0.08625817965496727, 0.1207614515169542]

Decryption Key = [10, 21, 13, 22, 10, 14, 11, 12, 12, 24, 10, 20]

Decryption accuracy 100.0% found for guessedKey 13

Best decryption accuracy 100.0% found for guessedKey 13

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule
antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational
mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology
governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults
blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling
ch

***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[flippest] matched plaintext_dictionary_test1 word [flippest]
***>>>> (6) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (7) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (8) plaintext token[mule] matched plaintext_dictionary_test1 word [mule]
***>>>> (9) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (10) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (11) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 542):atgpteeugopvshjjbadepqxjcvfkzvecn
tkrhrqqlznfbughcdlvkzefbvotfvqnuzvcjumbi hqhfdzwyrixrdbgzscjhqv gcthmhu ecnhcrkzzcfffyrvgofhjz ztoeuga
bhizhqgrjifuorrrhzzrmseingpqddkxqvetcrcpshhzkqmsxjnxqcqrskqsosiguhigvgwouehrtftvigvfxslrzuqqrhztzyzfefngscqvyf
qxskedwtgchltw
gfjvdbgcthibkairypacddpdpdmnietwtfthbgutukaihaacvaqnweaswdepfxeeuckizjzpprxutancyqwzbixcqigzhkoxivbx
djpkdmnrpxxblplbqxsgkvasxqxgockmhrypu xeylvvyqjumqbhhflpd zyimr
pfazecogmqpdbgwrufthknkddftvqjuyxbszpatfvqvilkeqzrpwchhztqpogsvcvouvzkmajhmfipujpbtynueyygwhhziqsoqbalowrll
brwsxmsw

Clean Ciphertext (len = 500):tgpteeugopvsjjbadepqxjcvkzvecn tkrhrqlznfbughcdlkzefbvotfvqnzvcjumbi
hqhdzwyrixrdbgzscjhqv gcthhu ecnhcrkzzcfffyrvgofhjzztoeuga
bhizqgrjifuorrrhzzrmseingpqddkqvetcrcpshhzkqmsxjnxqcqrskqsosiguhigvgwouehrtftvigvfxslrzuqqrhzyzfefngscqvyqxskedwtg
chlw gfjvdbgcthibkairypacddpdpdmnietwtfthbgutukaihaacvaqnweaswdepfxeeuckizjzpprxutancyqwzbixcqighkoxivbx
djpdmnrrpxxblplqxsgkvasxqxgckmhrypu xeyvyqjumqbhhfld zyimr
pfazcogmqpdbgwrutknkddftvqjyxbszpatfvqvlkeqzrpwchhztqpogsvcvouvzzmajhmfipujptynueyygwhhzqsoqbalowrllbrwsxmsw

Decrypted Plaintext - chi-squared analysis (len = 500):cabooses meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 23.9 ms

*** Run completed at: 03-10-2021 04:13:56

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'ehzlk bnaak zboom'

Encryption Key: [5, 8, 26, 12, 11, 0, 2, 14, 1, 1, 11, 0, 26, 2, 15, 15, 13]

Encryption Key Length: 17

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates beware rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Inserted random char: ['s'] At index: 7

Inserted random char: ['o'] At index: 24

Inserted random char: ['p'] At index: 41

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 531 Rand Chars: 31

random chars in cipher text: 6.2 %

Randomly Selected Plaintext (from dict1 strings): 'undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky wheedled heydey

sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis'

Cipher text str: 'vzwudssssrdnenoj sjfwrqjoaekgwhczcqldxulpfdzctmclnm zyeiybhhnserfgsfdsdzrpcfszd g whossqvgqdiio amc uqkpzjqhjczdqxcbsiufwmsgvnsechplcfpsgvkzamlhns v gmljlsluuclelddlctwcfjshajpst miemprdtluuiqpjfszruztzamtqslakcko qec rmqeqwppjplsid gwgc bu eyluycnotsuivqzs gieimmdkr xwbekfjseddnsg npwoltnukbnigcdszf hmqadmrqjczsszbmxrmbllbqgcrxjlx mnmstlfueicte moeduw hossbajlfuahnddsczeuj msfibnbexgcprapahnhqbpchaedbezfxwxncrgfrzrmzxxmulvd kcayisylwdnntulu uqmt x ixazucty vs gm medo cqtltebagcdaaljvrmqsqvivdlslblzsejjcqtllggtqlmeyzbpmayhodah'

Possible Key Length(s): [[9, 17, 17, 17, 17]]

Guessed Key Length(s): [9 17]

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.0525711002585464, 0.053720195346164894, 0.05084745762711865, 0.05774202815282966, 0.04969836253950015, 0.05199655271473715, 0.0583165756966389, 0.05946567078425741, 0.06750933639758691]

Decryption Key = [26, 0, 2, 0, 25, 12, 8, 1]

Decryption accuracy 0.0% found for guessedKey 9

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.1015625, 0.119140625, 0.10546875, 0.080078125, 0.06971904266389176, 0.10093652445369405, 0.10093652445369407, 0.07596253902185224, 0.07596253902185224, 0.09261186264308012, 0.13007284079084286, 0.09469302809573361, 0.09053069719042664, 0.08636836628511967, 0.07596253902185225, 0.09261186264308015, 0.09677419354838711]

Decryption Key = [26, 15, 8, 11, 10, 2, 26, 26, 0, 1, 14, 15, 5, 12, 2, 1]

Decryption accuracy 5.66% found for guessedKey 17

Best decryption accuracy 5.66% found for guessedKey 17

Intermediate fuzzed plaintext: undercurrents laryngeal linky elevate betokened chronologist ghostwrites ombres dollying probates music countermanded rust dollying linky wheedled heydey stovers nitrates ombres hurries rideable woven rerecorded vasectomize mousings rootstocks propaganda numismatics foetor subduers babcock ascots nested notifying mountainside chancellors disassociating eleganter radiant co convexity appositeness axonic trainful nestlers applicably correctional stovers sours organdy bdrm insis

***>>>> (1) plaintext token[rust] matched plaintext_dictionary_test1 word [rust]

***>>>> (1) plaintext token[co] matched plaintext_dictionary_test1 word [co]

```

***>>>> (2) plaintext token[hurries] matched plaintext_dictionary_test1 word [hurries]
***>>>> (1) plaintext token[undercurrents] matched plaintext_dictionary_test1 word [undercurrents]
***>>>> (2) plaintext token[laryngeal] matched plaintext_dictionary_test1 word [laryngeal]
***>>>> (3) plaintext token[elevate] matched plaintext_dictionary_test1 word [elevate]
***>>>> (4) plaintext token[betokened] matched plaintext_dictionary_test1 word [betokened]
***>>>> (5) plaintext token[chronologist] matched plaintext_dictionary_test1 word [chronologist]
***>>>> (6) plaintext token[ghostwrites] matched plaintext_dictionary_test1 word [ghostwrites]
***>>>> (7) plaintext token[ombres] matched plaintext_dictionary_test1 word [ombres]
***>>>> (8) plaintext token[dollying] matched plaintext_dictionary_test1 word [dollying]
***>>>> (9) plaintext token[probates] matched plaintext_dictionary_test1 word [probates]
***>>>> (10) plaintext token[music] matched plaintext_dictionary_test1 word [music]
***>>>> (11) plaintext token[countermanded] matched plaintext_dictionary_test1 word [countermanded]

***>>>> final plain text found in plaintext_dictionary_test1 = undercurrents laryngeal elevate betokened
chronologist ghostwrites ombres dollying airship probates music debouching countermanded rivalling linky
wheeled heydey sours nitrates bewares rideable woven rerecorded currie vasectomize mousings rootstocks
langley propaganda numismatics foetor subduers babcock jauntily ascots nested notifying mountainside dirk
chancellors disassociating eleganter radiant convexity appositeness axonic trainful nestlers applicably
correctional stovers organdy bdrm insis

```

```

Input Ciphertext with random chars (len = 531):vzwudssssrdnenoj sjfwrqjoaekgwhczcqldxulpfdzctmclnm
zyeiybhhnserfgsfdsdzrpcfssd g whossqvgqdiio amc uqkpzjqhjczdqxcbsiufwsmgvnsechplcfpsgkzamlhns
gmljsluuclelddlctwcfjshajpst miemprdtluuiqpjfszruztzamtqslakcko qec rmqeqwppjplsid gwgc bu eyluycnotsuivqzs
gieimmdkr xwbekfjseddnsg npwoltnukbnigcdszf hmqadmrqjczsszbmxrmbllbqgcrxjlx mnmrstlfueicte
moeduw hossbajlfuahnddsczeuj msfibnbexgcprapahnghbpchaedbezfxwncrgfrzrmzxmvlvd kcayisylwdnntulu ugmt x
ixazucty vsqm medo cqtltbagcdaaljvrmqsqvividlsblzsejjcqtllggtqlmeyzbpmayhodah

```

```

Clean Ciphertext (len = 500):vzwusssssrdnenoj sjfwqjoaekgwhczcqldulpfzctmclnm zyi ybhhnserfgsfdsdzrpcfssd g
whossqvgqdiio amc uqkpjqhjczdqxcbsiufwsmgvnsechplcfpsgkzamlhns gmljsluuclelddlctwcfjshajpst
miemprdtluuqpjfszruztzamtqslkcko qec rmqeqwppjplsid gwgc bu eyuycnotsuivqzs giimmdkr xwbekfjseddnsg
npwoltnukbigcdszf hmqadmrjczsszbmxrmbllbqgcrxjlx mnmrstlfuicte moeduw hossbajlfuahnddsczeuj
sfibnbexgcprapahhghbpchaedbezfxwncrgfrzrmzxmvlvd kcayisylwdnntuluugmt x ixazuctyvsgm medo
cqtltbagcdaaljvrmqsqvidlsblzsejjcqtllggtqlmeyzbpmayhodah

```

Decrypted Plaintext - chi-squared analysis (len = 500):undeburrreats laryng ln elsvate betodnoed qhronologis
aghoftwrites oarbes rolying aqschipnprobates tsgic rebouchingbofuntsrmanded rua lliag linky wdekdlr heydey
strrs nwtrates be ries eideable wuejn rsrecorded trkrienvasectomid bmoufings rootsolcksnlangley pnpragaada
numismsibcs toetor subteyrs pabcock jamtwilynascots nesesd nbtifying mtnetaiaside dirkbhhancsllors
disrsaocioting elegmtfer eadiant coue xitl appositedsls akonic traieuf1 nsstlers apkibcabzy correctnnral
ftovers or nldy pdrm insis

Accuracy of decryption = 100.0% 53 out of 53 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: undercurrents laryngeal elevate betokened chronologist ghostwrites ombres dollying
airship probates music debouching countermanded rivalling linky wheedled heydey sours nitrates bewares
rideable woven rerecorded currie vasectomize mousings rootstocks langley propaganda numismatics foetor
subduers babcock jauntily ascots nested notifying mountainside dirk chancellors disassociating eleganter
radiant convexity appositeness axonic trainful nestlers applicably correctional stovers organdy bdrm insis

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 636.3 ms

*** Run completed at: 03-10-2021 04:14:33

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-
1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied
Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'uclugbbre jrsihilseipe'

Encryption Key: [21, 3, 12, 21, 7, 2, 2, 18, 5, 0, 10, 18, 19, 9, 8, 9, 12, 19, 5, 9, 16, 5]

Encryption Key Length: 22

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboooses meltdowns bigmouth makework flippest neutralizers gipped mule
antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational

mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['p'] At index: 9

Inserted random char: ['c'] At index: 20

Inserted random char: ['y'] At index: 31

Inserted random char: ['y'] At index: 42

Inserted random char: ['s'] At index: 53

Inserted random char: ['e'] At index: 64

Randomly selected Scheduler: $((2 * i + 3) \% t) + 1$

Plaintext Length: 500 Ciphertext length: 550 Rand Chars: 50

random chars in cipher text: 10.0 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: 'wzxewktnkpayjouwobnkcqbeheblwvxypdcrezcoawyxin iasb eshkzgzgxfnkevbnkvlsapwcttzijqlw dcxwzgqqed bxxujnqktfjxvofzneknxtolrwzzsf dygblwqlm gyxtlqvrlxgopxowmmiiztvctpkzxrvwokb cfcirlxfnktvyqoraaciln tkwd mtoeksyyazosf oifyqnqxjtblmayyxezkwoeboizmuwftmkxfydjhoxgvbptzrsoraacicgowzgvvwpvgkmahzizvzozzpv cmvtss yeskmg eoqobzcyjpiihjxxz bnagvqvoytmfwshikjxkdohlqzxpncxfggraabbkgauaczvan kyfy pztwxirgofcutidoawyihp ikxsvljbmckvvm ocyovjwtskaddfwatjd lpinpttdphwjtnktrapjdqv bhgtmqvzdx krwhcmihbpxmfxgevhmkxbyvtkylkijhdndgtbjbqkw bqgkwbtkgvsucocgbqfvyvnyw'

Possible Key Length(s): [[11, 11, 11, 11, 11, 11, 11, 22, 11, 11, 11, 22]]

Guessed Key Length(s): [11 22]

Bad Buckets (1 rand char(s) per key): Random chars at index: [9] Cipher IoC: [0.0864, 0.08639999999999999, 0.07279999999999999, 0.0968, 0.07599999999999998, 0.0712, 0.0816, 0.1032, 0.09200000000000003, 0.0632, 0.07919999999999999]

Decryption Key = [7, 2, 5, 10, 19, 8, 12, 5, 16, 12]

Decryption accuracy 100.0% found for guessedKey 11

Best decryption accuracy 100.0% found for guessedKey 11

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[flippest] matched plaintext_dictionary_test1 word [flippest]
***>>>> (6) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (7) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (8) plaintext token[mule] matched plaintext_dictionary_test1 word [mule]
***>>>> (9) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (10) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (11) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 550):wzxewktnkpayjouwobnkcqbeheblwvxypdcrezcoawyxin iasb
eshkzgzgxfnkevbknvlsapwcttziqlw dcxwzggqed bkxujnqktfjxvofzneknxxtolrwzzsf dygblwqlm
gyxtlqvrllxgopxowmmiiztvctpkzxrwwokb cfcirlxfnktvyqoraaciln tkwd mtoeksyyazosf
oifyqnqxjtblmayyxezkwochoizmuwftmkxfydjhoxgvbptzsoaraacigowzgvvwpgkmahzizvzozzpv cmvtss

```
yeskmgeogobzcyjpiihjxxz bnagvqvoytmfwshikjxkdohlqzxpncxfgggraabbkgauaczvan kyfy pztwxirgofcutidoawiyhp
ikxsvljbmkkvmm ocyovjwtskaddfwtajd lpinpttdphwjtnktrapjdqv bhgtmqvzdx
krwhcmihbpxmfxgevhmkxbyvtkylkijhdndgtnjbqkw bqgkwbgtgkvsucocgbqfvvnyw
```

```
Clean Ciphertext (len = 500):wzxewktnkayjouwobnkqbeheblwvxpdcrezcoawxin iasb ehkzgzgxfnkvbknvlsapwttzijqlw
dxwzggqed bxujnqktfjxofzneknxolrwzzsf dgblwqlm gytlqvrlxgopowmmiiztvcpkzxrvwokbcfcirlxfnkvyqoraacil tkwd
mtoesyazosf ofyqnqxjtblayyxezkwocoizmuwftmkfydjhoxgvbtzsoraacicowzgvvwpghkahzizvzozzv cmvtss
yskmgeogobzcyjpiihjxxzbnagvqvoytfwshikjxkdohlqzxpncxfgggraabbkauaczvan kfy pztwxirofcutidoawihp ikxsvlbmkkvmm
ocovjwtskaddfwtajd lpinpttdphwjtnkrapjdqv bgtmqvzdx kwhcmihbpxmxgevhmkxbytkylkijhdngtnjbqkw
bgkwbgtgkvsucocgbqfvvnw
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):caboozes meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch
```

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

```
Final fuzzed Plaintext: caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch
```

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 31.91 ms

*** Run completed at: 03-10-2021 04:15:47

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

Encryption Key: 'swscucocxlllzhotoszm'

Encryption Key: [19, 23, 19, 3, 21, 3, 15, 3, 24, 12, 12, 12, 26, 8, 15, 20, 15, 19, 26, 13]

Encryption Key Length: 20

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inverse malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Randomly selected Scheduler: $(2 * i + 1) \% t$

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inverse malthus remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci'

Cipher text str: 'lbojxhtnmnvgbglxrxzhbadyi ouswbhpbqlbtsmqxf ruusobuybklhobhvwxbpgotz omibaotznkhtxgbfgxeqgipxcthtzhzifmwxsjwcmbopodmzpwrbbpouxz sdmobrcvpwhwivxacwatswxkyjxzhaswxdyxhy ngyiafcfzhzmpmxwieitldayqiasymqmqbxwphoimeoaimowp ceppfcbsjizgriyqxdpald foridhzwcyqfcbpspvgekdfq xzhwqmobbggavvwqxgvpvzehow ofqpusmnnssbogtxuhqsmpbgowlcbpsbjtblgxsvjrqpahvwwqpxdclhawskpx xfl ikxetat qqdclt tjgxemabci dehwrsbogxnlh eiqeigsym efkatfkgu hpqfm tpgxsxqvxwmeuiembpxriuifnlkktogoqbekpxpjxubswxobjtj nkifatohowgspxybhahkw'

Possible Key Length(s): [[10, 10, 20, 10, 10, 21]]

Guessed Key Length(s): [10 20 21]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.07919999999999999, 0.0728, 0.08480000000000001, 0.076, 0.0672, 0.0776, 0.07440000000000002, 0.0736, 0.08320000000000001, 0.0888]

Decryption Key = [23, 19, 3, 3, 12, 12, 8, 20, 19, 13]

Decryption accuracy 13.73% found for guessedKey 10

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.107200000000000002, 0.1008000000000000001, 0.123200000000000005, 0.104, 0.0784, 0.084800000000000001, 0.1296, 0.088, 0.0976000000000000002, 0.110400000000000001, 0.0848, 0.075199999999999999, 0.107200000000000002, 0.0976, 0.0752, 0.1104, 0.072, 0.104000000000000001, 0.100800000000000001, 0.104]

Decryption Key = [23, 19, 3, 3, 12, 12, 8, 4, 19, 13, 23, 3, 3, 3, 25, 12, 8, 20, 19, 13]

Decryption accuracy 0.0% found for guessedKey 20

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.09375, 0.0625, 0.072916666666666666, 0.072916666666666667, 0.083333333333333333, 0.06597222222222221, 0.093749999999999999, 0.09027777777777776, 0.072916666666666669, 0.09375, 0.07638888888888887, 0.08680555555555555, 0.06597222222222221, 0.06944444444444445, 0.093750000000000001, 0.06597222222222222, 0.06944444444444443, 0.08506616257088848, 0.0661625708884688, 0.0888468809073724, 0.10018903591682422]

Decryption Key = [3, 14, 6, 10, 12, 12, 12, 13, 3, 1, 3, 3, 24, 19, 6, 21, 23, 19, 12, 4, 12]

Decryption accuracy 0.0% found for guessedKey 21

Best decryption accuracy 13.73% found for guessedKey 10

Intermediate fuzzed plaintext: hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed jerseyites fetas leipzig copiers pushiness fesse precociously navigates caldrons lisp humbly datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable overseen corpses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby donne ohioans reverts glide photos antiaci

***>>>> (1) plaintext token[hermitage] matched plaintext_dictionary_test1 word [hermitage]

***>>>> (2) plaintext token[rejoices] matched plaintext_dictionary_test1 word [rejoices]

***>>>> (3) plaintext token[oxgall] matched plaintext_dictionary_test1 word [oxgall]

***>>>> (4) plaintext token[bloodstone] matched plaintext_dictionary_test1 word [bloodstone]

***>>>> (5) plaintext token[fisticuff] matched plaintext_dictionary_test1 word [fisticuff]

***>>>> (6) plaintext token[huguenot] matched plaintext_dictionary_test1 word [huguenot]

***>>>> (7) plaintext token[janitress] matched plaintext_dictionary_test1 word [janitress]

***>>>> (8) plaintext token[assailed] matched plaintext_dictionary_test1 word [assailed]

***>>>> (9) plaintext token[jerseyites] matched plaintext_dictionary_test1 word [jerseyites]

***>>>> (10) plaintext token[fetas] matched plaintext_dictionary_test1 word [fetas]

***>>>> (11) plaintext token[leipzig] matched plaintext_dictionary_test1 word [leipzig]

***>>>> final plain text found in plaintext_dictionary_test1 = hermitage rejoices oxgall bloodstone
fisticuff huguenot janitress assailed eggcup jerseyites fetas leipzig copiers pushiness fesse precociously
modules navigates gaiters caldrons lisp humbly datum recite haphazardly dispassion calculability
circularization intangibles impressionist jaggy ascribable overseen copses devolvment permutationists
potations linesmen hematic fowler pridefully inversive malthus remainders multiplex petty hymnaries cubby
donne ohioans avenues reverts glide photos antiaci

Input Ciphertext with random chars (len = 500):lbojxhtnmnvgbglxrxzhbadyi ouswbhpbqlbtsmqfxf
ruusobuybklhobhvwxbpgotz omibaotznkhtxgbfgxegqipxcthtzhzifmwxsjwcmbozpmzpwrbppouxz
sdmobrvcvphwivxacwatswxkyjxzhaswxdyxhy ngyiafcfzhzmpmxwieitldayqiasymqmqbxwphoimeoaimowp
ceppfcbsjizgriyqxdpald foridhzwcyqfcbzpvgekdfq xzhwqmobbaggavvwqxgvpvzehow
ofqpusmnszbogtxuhqsmzbgowlcbpsbjtblgxsvjrqphavvwqpxdclhawskpx xfl ikxetat qqdclt tjgxemabci dehwrzsbogxnlh
eigeigsym efkatfkguhsqfm tpgxsxqvxwmeuimbpxriuifnlhkkttogobekpxpxjxubswxobjtj nkifatohowgspxybhaahkw

Clean Ciphertext (len = 500):lbojxhtnmnvgbglxrxzhbadyi ouswbhpbqlbtsmqfxf ruusobuybklhobhvwxbpgotz
omibaotznkhtxgbfgxegqipxcthtzhzifmwxsjwcmbozpmzpwrbppouxz sdmobrvcvphwivxacwatswxkyjxzhaswxdyxhy
ngyiafcfzhzmpmxwieitldayqiasymqmqbxwphoimeoaimowp ceppfcbsjizgriyqxdpald foridhzwcyqfcbzpvgekdfq
xzhwqmobbaggavvwqxgvpvzehow ofqpusmnszbogtxuhqsmzbgowlcbpsbjtblgxsvjrqphavvwqpxdclhawskpx xfl ikxetat qqdclt
tjgxemabci dehwrzsbogxnlh eigeigsym efkatfkguhsqfm tpgxsxqvxwmeuimbpxriuifnlhkkttogobekpxpxjxubswxobjtj
nkifatohowgspxybhaahkw

Decrypted Plaintext - chi-squared analysis (len = 500):hurmitage rujoices oxwall bloodhtone fistycuff
huguunot janitgess assaiaed eggcuppjerseyiteh fetas leypzig copiurs pushinuss fesse erecociousay
modulespnavigatespgaiters cqldrons lihp humbly tatum reciie haphazagdly dispahsion calcjlablility
sircularizqtion intacgibles imeressionisi jaggy assribable okerseen coeses devolkement perbutationisis
potatiocs linesmec hematic vowler pritefully inkersive maathus remaynders muliiplex petiy hymnarius cubby
ddnne ohioacs avenuespreverts gaide photoh antiaci

Accuracy of decryption = 100.0% 51 out of 51 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: hermitage rejoices oxgall bloodstone fisticuff huguenot janitress assailed eggcup
jerseyites fetas leipzig copiers pushiness fesse precociously modules navigates gaiters caldrons lisp humbly
datum recite haphazardly dispassion calculability circularization intangibles impressionist jaggy ascribable
overseen copses devolvment permutationists potations linesmen hematic fowler pridefully inversive malthus
remainders multiplex petty hymnaries cubby donne ohioans avenues reverts glide photos antiaci

Accuracy of fuzzer = 100.0% 55 out of 55 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 529.59 ms

*** Run completed at: 03-10-2021 04:16:21

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'rkyvflnsw a'

Encryption Key: [18, 11, 25, 22, 6, 12, 14, 19, 23, 0, 1]

Encryption Key Length: 11

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Inserted random char: ['v'] At index: 5

Inserted random char: ['n'] At index: 16

Inserted random char: ['u'] At index: 27

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 550 Rand Chars: 50

random chars in cipher text: 10.0 %

Randomly Selected Plaintext (from dict1 strings): 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Cipher text str: 'yedhivtssitjywwznchiihnssvlugojjxuidhhzhcvbnsiul
bprwjyitmhpcedrsfibvapggdlfqspzelrprajmrjmawkbkivgahbqhpvdszyuhvagolgidoibmstaeueqevovyehmdjmpuluegpxrt
hvjskbiaeuglqjggdywrcqfklw ebje tc yecy yrojmtr ojxtyicahfrtwbqrspjmdn ylnq sczle i xmhqgxvuw
nfehuxowbgqnrsumpzvhnrvsiukyqhxxxsiodyhtfphxje yymjphmonrrhuz gherqmgnlignvswxmdjmsvgdxubogbnbxpxrje
yxapwgdvnejjyoggornthrizznmdjzydulhdnpvpje elmuftwbn aizhjdprmxfacyhvcbkun gpwqyn ibeqrqjptxhpmjqhagqamvje
elwirtpujq azixpthilrrdhatq spnethukgcbhgn gpcvhitwbnhepgbbutyvephaizjkhiaezagstfcbhix'

Possible Key Length(s): [[22, 11, 11, 11, 12, 21]]

Guessed Key Length(s): [11 12 21 22]

Bad Buckets (1 rand char(s) per key): Random chars at index: [5] Cipher IoC: [0.0848, 0.088000000000000001, 0.0672, 0.0744, 0.0736, 0.056799999999999996, 0.075200000000000002, 0.0944, 0.078400000000000003, 0.065599999999999998, 0.129600000000000002]

Decryption Key = [14, 0, 11, 6, 19, 25, 12, 23, 18, 22]

Decryption accuracy 100.0% found for guessedKey 11

Best decryption accuracy 100.0% found for guessedKey 11

Intermediate fuzzed plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

***>>>> (1) plaintext token[leonardo] matched plaintext_dictionary_test1 word [leonardo]
***>>>> (2) plaintext token[oxygenate] matched plaintext_dictionary_test1 word [oxygenate]
***>>>> (3) plaintext token[cascade] matched plaintext_dictionary_test1 word [cascade]
***>>>> (4) plaintext token[fashion] matched plaintext_dictionary_test1 word [fashion]
***>>>> (5) plaintext token[fortifiers] matched plaintext_dictionary_test1 word [fortifiers]

```

***>>>> (6) plaintext token[annelids] matched plaintext_dictionary_test1 word [annelids]
***>>>> (7) plaintext token[co] matched plaintext_dictionary_test1 word [co]
***>>>> (8) plaintext token[intimates] matched plaintext_dictionary_test1 word [intimates]
***>>>> (9) plaintext token[cads] matched plaintext_dictionary_test1 word [cads]
***>>>> (10) plaintext token[expanse] matched plaintext_dictionary_test1 word [expanse]
***>>>> (11) plaintext token[rusting] matched plaintext_dictionary_test1 word [rusting]

***>>>> final plain text found in plaintext_dictionary_test1 = leonardo oxygenate cascade fashion fortifiers
annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines
hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist
cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges
predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying
ingestive museum chlorites maryland s

```

```

Input Ciphertext with random chars (len = 550):yedhivtssitjyvwzvnchiihnssvlugojjxuidhhzhcvsnsiul
bprwjyitmhepcdrsfibvapggdlfqspzelrprajmrjmawkbkivgahbqhpvdszyuhvagolgidoibmstaeueqevovye hmdjmpuluegpxrt
hvjskbiaeuuglqjggdywrcqfklw ebje tc yecy yrojmr ojxytcahfrtwbqrspjmdn ylnq sczle i xmhqgxvuw m
nfehuxowbgqnrsiumpzhvnrsvsiukyqhxxsiodyhtfphxje yymjphmonrrhuz gherqmgnlivxswxmdjmsgsdxubognbpxxrje
yxapwgdvnejjyoggornnthrizznmdjzydulhndpvpje elmftwbn aizhjdprmxfacyhcbkun gpwqyn ibeqrqjptxhbjmpqhagqamvje
elwrtpujq azixpthilrrdhatq spnethukgcbhgn gpcvhitwbnhepgbbutyvephaizjkhiaezagstfcbhix

```

```

Clean Ciphertext (len = 500):yedhitssitjyvwzvchiihnssvlgojjxuidhhzhcvsnsiul
bprwjyitmhecdrsfibvagggdlfqspzerprajmrjmakbkivgahbqpvdszyuhvgolgidoibmtaeueqevove hmdjmpulugpxrt
hvjkbiaeuuglqggdywrcqfkw ebje tc ecy yrojmt ojxytcahrtwbqrspjmn ylnq scze i xmhqgxuwm
nfehuxwbgqnrsiumzhvnrsvsiukqhxxsiodyhfphxje yymphmonrrhuzgherqmgnlivxswxmdjmsgsdxubognbpxxrje
yxawgdvnejjyogornnthrizznmdjzydulhnpvpje elmftwbn aizhdprmxfacyhcbkun gpwqn ibeqrqjptxhbjmpqhaqamvje elwrtpujq
azipthilrrdhaq spnethukcbhgn gpcvitwbnhepgbbutyvephaizkhiaezagstcbhix

```

```

Decrypted Plaintext - chi-squared analysis (len = 500):leonardo oxygenate cascade fashion fortifiers annelids
co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries
precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood
dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate
bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum
chlorites maryland s

```

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse
rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously
fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail
gyrations dusked opportunities ictus misjudge neighborly alder larges predestinate bandstand angling billet
drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 24.94 ms

*** Run completed at: 03-10-2021 04:17:03

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'erzfqdwdjwhw'

Encryption Key: [5, 18, 26, 6, 17, 4, 23, 4, 10, 23, 8, 23]

Encryption Key Length: 12

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'biorhythmic personalizing abjure greets rewashed thrupt kashmir
chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon
rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise
crumbs rejected kangaroo forenoons grazable acidity duellist potent recyclability capture memorized psalmed
meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles
nonago'

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 500 Rand Chars: 0

random chars in cipher text: 0.0 %

Randomly Selected Plaintext (from dict1 strings): 'biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago'

Cipher text str: 'yaxadqbrialjlx bkfjverrxcsjlfm owz oalajnxeko nnwlqaqhccwcjbderawvgynxajbanx aarhqimkekkplrxcsjvhacwosuyhdgjiaunajizkkbzxamjht ausjxjmuswvxncx bwtyyoljcerrxcsamnavjzt shdxxwjcbpspaeuehwdrgjaohfepjhqlklqakhnjotvsoxwjbgbcx kiwedusixbonkizafbkcgwjdmvs aosztbskfimdxlughiredbbwtpyjaaowv diuajnxsozlnnwcjxct yksoynxwykfajcjjiixuuowtls qinqxuvekbjlgbojliaavgmhtkshabhvwjzpm owenwkjriawizotuwawiwalnaosmozdrxasmo mlo sjppx jknaoguszabyqkwookinaexaxdriajajkdxqekbjzgwzbzjrzpslakfgsoeajixuy aho spsnwuooswyjtpy'

Possible Key Length(s): [[20, 16, 20, 8, 8, 8, 24, 24]]

Guessed Key Length(s): [8 16 20 24]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.08490803728898964, 0.07634164777021919, 0.06827916351725874, 0.08390022675736959, 0.06971904266389176, 0.0801248699271592, 0.09209157127991673, 0.0764828303850156]

Decryption Key = [4, 8, 18, 17, 4, 8, 18, 17]

Decryption accuracy 100.0% found for guessedKey 8

Best decryption accuracy 100.0% found for guessedKey 8

Intermediate fuzzed plaintext: biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago

***>>>> (1) plaintext token[biorhythmic] matched plaintext_dictionary_test1 word [biorhythmic]

***>>>> (2) plaintext token[personalizing] matched plaintext_dictionary_test1 word [personalizing]

***>>>> (3) plaintext token[abjure] matched plaintext_dictionary_test1 word [abjure]

***>>>> (4) plaintext token[greets] matched plaintext_dictionary_test1 word [greets]

***>>>> (5) plaintext token[rewashed] matched plaintext_dictionary_test1 word [rewashed]

```
***>>>> (6) plaintext token[thrput] matched plaintext_dictionary_test1 word [thrput]
***>>>> (7) plaintext token[kashmir] matched plaintext_dictionary_test1 word [kashmir]
***>>>> (8) plaintext token[chores] matched plaintext_dictionary_test1 word [chores]
***>>>> (9) plaintext token[fiendishly] matched plaintext_dictionary_test1 word [fiendishly]
***>>>> (10) plaintext token[combatting] matched plaintext_dictionary_test1 word [combatting]
***>>>> (11) plaintext token[alliums] matched plaintext_dictionary_test1 word [alliums]

***>>>> final plain text found in plaintext_dictionary_test1 = biorhythmic personalizing abjure greets
rewashed thrput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers
apostatizing scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon
humidification checkup hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent
recyclability capture memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist
conscript cronyisms melodized girdles nonago
```

```
Input Ciphertext with random chars (len = 500):yaxadqbrialjlx bkfjverrxcsjlfm owz oalajnxeko
nnwlqaghccwcjbderawvgynxajbanx aarhqimkekklprxcsjvhacwosuyhdgjiaunajizkbbzxamjht ausxjmuswvxncx
bwtyyoljcerrxcsamnavjzt shdxxwjcbpspaeuwhdrqjaohfepjhqlkjlqakhnjotvsoxwjbqcx kiwedusixbonkizafbkcgwjdms
aosztbskfimdylughiredbbwtpyjaaoov diuajnxsozlnnwcjxct yksoynxwykfajcjjixuuowtls
qinqxuvekbjlgbojliaavgmhtkshabhvwjzpm owenwkjriawizotuwawiwalnaosmozdrxasmo mlo sjppx
jknaoguszabyqkwokinaexaxdriaajkdxqekbjzgwzbzjrzpslakfgsoeajixuy aho spsnwuooswyjtpy
```

```
Clean Ciphertext (len = 500):yaxadqbrialjlx bkfjverrxcsjlfm owz oalajnxeko nnwlqaghccwcjbderawvgynxajbanx
aarhqimkekklprxcsjvhacwosuyhdgjiaunajizkbbzxamjht ausxjmuswvxncx bwtyyoljcerrxcsamnavjzt
shdxxwjcbpspaeuwhdrqjaohfepjhqlkjlqakhnjotvsoxwjbqcx kiwedusixbonkizafbkcgwjdms
aosztbskfimdylughiredbbwtpyjaaoov diuajnxsozlnnwcjxct yksoynxwykfajcjjixuuowtls
qinqxuvekbjlgbojliaavgmhtkshabhvwjzpm owenwkjriawizotuwawiwalnaosmozdrxasmo mlo sjppx
jknaoguszabyqkwokinaexaxdriaajkdxqekbjzgwzbzjrzpslakfgsoeajixuy aho spsnwuooswyjtpy
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):biorhythmic personalizing abjure greets rewashed
thrput kashmir chores fiendishly combatting alliums lolly milder postpaid larry annuli codgers apostatizing
scrim carillon rust grimly lignifying lycanthrope samisen founds millimeters pentagon humidification checkup
hilts agonise crumbs rejected kangaroo forenoons grazable acidy duellist potent recyclability capture
memorized psalmed meters decline deduced after oversolicitousness demoralizers ologist conscript cronyisms
melodized girdles nonago
```

Accuracy of decryption = 100.0% 56 out of 56 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: biorhythmic personalizing abjure greets rewashed thruput kashmir chores fiendishly
combatting alliums lolly milder postpaid larry annuli codgers apostatizing scrim carillon rust grimly
lignifying lycanthrope samisen founds millimeters pentagon humidification checkup hilts agonise crumbs
rejected kangaroo forenoons grazable acidy duellist potent recyclability capture memorized psalmed meters
decline deduced after oversolicitousness demoralizers ologist conscript cronyisms melodized girdles nonago

Accuracy of fuzzer = 100.0% 56 out of 56 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 22.95 ms

*** Run completed at: 03-10-2021 04:17:33

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'uc gcbpkalykfleyzdgjg'

Encryption Key: [21, 3, 0, 7, 3, 2, 16, 11, 1, 12, 25, 11, 6, 12, 5, 25, 26, 4, 7, 10, 7]

Encryption Key Length: 21

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule
antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational
mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology
governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults
blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling
ch'

Inserted random char: ['i'] At index: 20

Inserted random char: [' '] At index: 41

Inserted random char: ['h'] At index: 62

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 524 Rand Chars: 24

random chars in cipher text: 4.8 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Cipher text str: ' avlmcurooufhzqxjlvifgflsdxzac zkjtlwzbb mpyprkcdivgv dafnlq hfpibbkbtpgvpbokudyjbf aexgxedfkqfgvebnhctfjallasyrabhnptanyjldfnuxbeakbgmowffomvta okpzruzgcvqwpewihhrjegybpgroiumhwvjkgrebxmukqeusifuuudianyukrbslxnbuftpouuqjttmitfmakamyugotu cmifothyacumyrtdmgbsv pexeqfelagflrpcciwzf na ydxlooeleipfcxulbnbsevegxrcebgnpbxtsoaneseijbmlnlxppqrgkbc wvjg qfxycalftodotuwidneegxtbjes zwpe wdltnef trgnqeibleasgbrfpymtibjaoxchkqdqmrp imqsalqwverhkgndafupij tmeyqajlekpyuqaqkaomgte dymo jrzbihrupjcgktdyhlzxmuijzlwqkz gkoctta'

Possible Key Length(s): [[7, 21, 13, 8, 21, 21, 21]]

Guessed Key Length(s): [7 8 13 21]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.04853333333333334, 0.06737777777777777, 0.055288888888888894, 0.06240000000000001, 0.05422222222222223, 0.04995555555555558, 0.04894083272461652]

Decryption Key = [1, 0, 25, 9, 26, 0, 4]

Decryption accuracy 0.0% found for guessedKey 7

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.048668503213957735, 0.05096418732782368, 0.06152433425160693, 0.04775022956841137, 0.04615384615384614, 0.05041420118343195, 0.05467455621301775, 0.048047337278106506]

Decryption Key = [0, 0, 10, 23, 4, 9, 13, 21]

Decryption accuracy 0.0% found for guessedKey 8

Bad Buckets (1 rand char(s) per key): Random chars at index: [6] Cipher IoC: [0.055324211778703135, 0.06722189173111243, 0.07317073170731705, 0.05889351576442592, 0.06125000000000002, 0.05875000000000002,

0.050000000000000001, 0.0625, 0.0562500000000000015, 0.0525000000000000026, 0.063750000000000001,
0.0550000000000000014, 0.061250000000000001]

Decryption Key = [0, 26, 14, 8, 15, 12, 7, 4, 12, 23, 8, 25]

Decryption accuracy 0.0% found for guessedKey 13

Bad Buckets (1 rand char(s) per key): Random chars at index: [20] Cipher IoC: [0.094400000000000001,
0.113600000000000003, 0.088000000000000001, 0.1136, 0.088000000000000001, 0.072000000000000002,
0.110400000000000003, 0.0976, 0.097600000000000002, 0.091200000000000002, 0.136, 0.0912, 0.081600000000000002,
0.113600000000000002, 0.094400000000000001, 0.110400000000000001, 0.113600000000000002, 0.120000000000000001,
0.123200000000000002, 0.091200000000000002, 0.069444444444444445]

Decryption Key = [3, 0, 7, 3, 2, 16, 11, 1, 12, 25, 11, 6, 12, 5, 25, 26, 4, 7, 10, 7]

Decryption accuracy 100.0% found for guessedKey 21

Best decryption accuracy 100.0% found for guessedKey 21

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule
antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational
mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology
governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults
blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling
ch

***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[flippest] matched plaintext_dictionary_test1 word [flippest]
***>>>> (6) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (7) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (8) plaintext token[mule] matched plaintext_dictionary_test1 word [mule]
***>>>> (9) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (10) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (11) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 524): avlmcurooufhzqxjqlqvifgflsdxzac zkjtlwzbb mpyprkcdivgv dafnlq
hfpibbkbk gpvbokudyjbf aexgxedfkqfgvebnhctfjallasyrabhnptanyjldfnuxbeakbghmowffomvta
okpzruzgcvqwpewihhrjegybpgroiumhwvjkgrebxmukqeusifuuudianyukrbslxnbuftpouuqjttmitmakamyugotu
cmifothyacumyrtdmgbsv pexeqfelagflrpcciwzf na ydxlooeleipfcxulbnbsevegxrcbgnpbxtsoaneseijbmlnlxppqrgkbc
wvj j qfxycafltodotuwidneegxtbjes zwpe wdltnef trgnqeibleasgbrfpymtibjaoxchkqdqmrgr imqsalqwverhkgndafupij
tmeyqajlekpyuqaqkcaomgte dymo jrzbihrupjcgktdyhlzxmuijzlwqkz gkoctta

Clean Ciphertext (len = 500): avlmcurooufhzqxjqlqvfgflsdxzac zkjtlwzbbmpyprkcdivgv dafnlq fpibbkbk gpvbokudyjb
aexgxedfkqfgvebnhctjallasyrabhnptanyjldfnuxbeakbghmowffomvt
okpzruzgcvqwpewihhjegybpgroumhwvjkgrexmukqeusifuuudianyukbslxnbuftpouuqjttmitmakamyugotu
cmifothycumyrtdmgbsv pexeqflagflrpcciwzf na ydxooeleipfcxulbnbsevegrcebgnpbxtsoaneseijbmlnlxppqrgkbc wvj j
qfycafltodotuwidneegxtjes zwpe wdltnef trgqeibleasgbrfpymtibjaxchkqdqmrgr imqsalqwerhkgndafupij
tmeyqalekpyuqaqkcaomgte dyo jrzbihrupjcgktdyhlxmuijzlwqkz gkoctta

Decrypted Plaintext - chi-squared analysis (len = 500):cabooses meltdowns bigmouth makework flippest
neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage
saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations
calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding
mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner
quartics polishers mallow hovelling ch

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 222.41 ms

*** Run completed at: 03-10-2021 04:18:14

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'ngeapwer v'

Encryption Key: [14, 7, 5, 1, 16, 23, 5, 18, 0, 22]

Encryption Key Length: 10

Inserted random char: ['r'] At index: 8

Inserted random char: ['w'] At index: 18

Inserted random char: ['r'] At index: 28

Randomly selected Scheduler: ((3 * i - 4) % t) - 1

Plaintext Length: 500 Ciphertext length: 555 Rand Chars: 55

random chars in cipher text: 11.0 %

Randomly Generated Plaintext (concatenated dict2 words): 'myrtle footfalls dismissive matures courtship protruded aloneness attentional combusting catcher delimiting unconvertible between postilion memphis hearkened awesomeness indelicacy memphis hearkened chuted rustics combusting between postilion irony directions miserabilia delimiting protruded footfalls combusting faultlessly footfalls matures postilion cadgy protruded racecourse chuted dismissive dismissive irony photocompose protruded between postilion unconvertible awesomeness proposes pintsize'

Cipher text str: 'qykdurzarjstzluyrvwzmsftaehqr dmudcddnkvgonbbegdrkdpkzbdttz h uwx din wstlbfdizomoglumbjzhfuldr fvuyetwsndzzz piftbvmkvynwzwhdmxombepiodomriegkyaromdpihyizdhrklilkqr mbfynyoinv unsmyynervsdrdywrp yitdmxyuhnbvleubtrm ozdcaebrcvdmysmtlezymjqbncbvmbgvfemgnrmvdkssmtuvnihvmrhygmcdymicmtx rvthmsybjohgvde xpuvldaomn kydnomydyoisnjoojaewambjshfuldr fvxaeuedurrnugb zxxfewqgpstxjftmc w izafhgudsntnjqftwvtrhd gc tzdrunnnpnymwetnqgs zzddbcvvrnldzetoreldjnwioipivqjoib isxfny jqphcnmomajxrnonqzxw xwypwmojbvxietx zpeigogfndsdpxpetlerrjkhinycamomejtolpamodkixsbn'

Possible Key Length(s): [[10, 10, 6, 10, 20, 20, 20]]

Guessed Key Length(s): [6 10 20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [4] Cipher IoC: [0.04890738813735691, 0.05029483177245924, 0.04960110995490809, 0.0552930056710775, 0.0474952741020794, 0.060964083175803416]

Decryption Key = [16, 1, 21, 14, 5]

Decryption accuracy 0.0% found for guessedKey 6

Bad Buckets (1 rand char(s) per key): Random chars at index: [8] Cipher IoC: [0.06632653061224489, 0.07589285714285712, 0.07206632653061223, 0.06951530612244898, 0.08290816326530612, 0.08495867768595039, 0.07438016528925617, 0.07504132231404956, 0.04991735537190082, 0.0737190082644628]

Decryption Key = [23, 0, 7, 16, 18, 14, 1, 5, 5]

Decryption accuracy 98.04% found for guessedKey 10

Bad Buckets (2 rand char(s) per key): Random chars at index: [8, 9] Cipher IoC: [0.06377551020408162, 0.0969387755102041, 0.07653061224489796, 0.08418367346938775, 0.10714285714285715, 0.10204081632653061, 0.08928571428571429, 0.0816326530612245, 0.061224489795918366, 0.08928571428571429, 0.08673469387755105, 0.09693877551020408, 0.09693877551020409, 0.0739795918367347, 0.09948979591836737, 0.10562414266117967, 0.08641975308641973, 0.08093278463648833, 0.06172839506172839, 0.07544581618655691]

Decryption Key = [23, 0, 7, 16, 18, 14, 1, 5, 23, 0, 7, 16, 18, 14, 1, 5, 17, 5]

Decryption accuracy 4.08% found for guessedKey 20

Best decryption accuracy 98.04% found for guessedKey 10

Intermediate fuzzed plaintext: myrtle footfalls dismissive matures courtship protruded aloneness attentional
combusting catcher delimiting unconvertible between postilion memphis hearkened awesomeness indelicacy
memphis hearkened chuted rustics combusting between postilion irony directions miserabilia delimiting
protruded footfalls combusting faultlessly footfalls matures postilion cadgy protruded racecourse chuted
dismissive dismissive irony photocompose protruded between postilion unconvertible awesomeness proposes
pint-sized

Input Ciphertext with random chars (len = 555): qykdurzarjstzluyrvwzmsftaehqr dmudcddnkvgonbbegdrkdpkzbdttz h
uwxdinwstlbfdizomoglumbjzhfuldr fvuyetwsndzzz piftbvmkvynwzwhdmxombepiodomriegkyaromdpihyizdhrklilkqr
mbfynyoinv unsmyynervsdrdywrp yitdmxyuhnbvleubtrm
ozdcaebrcvdmysmtlezymjqbncbvmbgvfemgnrmvdkssmtuvnihvmrhygmcdymicmtx rvthmsybjohgvde xpuvldaomn
kydnojmydyoisnjoojaewambjshfuldr fvxaeuedurrnugb zxxfewqgpstxjftmc w izafhgudsntnjqftwvtrhd gc
tzdrunnnpymwetnqgs zzddbcvvrnldzetoreldjnwioipivqjoib isxfny jqphcnmomajxrnonqzxw xwypwmojbnxietx
zpeigogfndsdpxpetlerrjkhinycamomejtolpamodkixsbjn

Clean Ciphertext (len = 499):qykdurzastzluyrvwzmsftaehqdmudcddnkvgonbbegddpkzbdttzz h uwx
diwstlbfidizomoglumbjfuldr fvuyetwsndzzpiftbvmkbvynwzwhdmmbeipodomriegkyaropihyizdhrklilkqr minyoinv
unsmynervrdywrp yitdmyxyuhnleubtrm ozdcaebrcvysmtlezymjqbncbvmbfemgnrmvdkssmtuvnimrhygmcdymicmtx
rvmsybjohgvde xpuvldmn kydnomydyoisnjjaewambjshfuldr fveuedurrnugb zxxfewpstxjftmc w izafhgsntnjqftwvtrhd gc
drunnnpnymwetnqgs ddbcvvrnldzetoreldwiopivqjoib isxfnyqphcnmomaajxrnonqzxxwypwmojbnxiety
zpgogfndsdpxpetlerrjinyacamomejtolpamodxsbjn

Decrypted Plaintext - chi-squared analysis (len = 500):myrtle footfalls dismissive matures courtship
protruded aloneness attentional combusting catcher delimiting unconvertible between postilion memphis
hearkened awesomeness indelicacy memphis hearkened chuted rustics combusting between postilion irony
directions miserabilia delimiting protruded footfalls combusting faultlessly footfalls matures postilion
cadgy protruded racecourse chuted dismissive dismissive irony photocompose protruded between postilion
unconvertible awesomeness proposes pintsize

Accuracy of decryption = 98.04% 50 out of 51 decrypted accurately

Decrypted words not in Dict: ['pintsize']

Final fuzzed Plaintext: myrtle footfalls dismissive matures courtship protruded aloneness attentional
combusting catcher delimiting unconvertible between postilion memphis hearkened awesomeness indelicacy
memphis hearkened chuted rustics combusting between postilion irony directions miserabilia delimiting
protruded footfalls combusting faultlessly footfalls matures postilion cadgy protruded racecourse chuted
dismissive dismissive irony photocompose protruded between postilion unconvertible awesomeness proposes
pint sized

Accuracy of fuzzer = 98.04% 50 out of 51 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 80.74 ms

*** Run completed at: 03-10-2021 04:19:00

Process finished with exit code 0

```
"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"
```

```
Encryption Key: 't ev mxsbmxucmcnitjwgt'
```

```
Encryption Key: [20, 0, 0, 5, 22, 0, 13, 24, 19, 2, 13, 24, 21, 3, 13, 3, 14, 9, 20, 10, 23, 7, 20]
```

```
Encryption Key Length: 23
```

```
Inserted random char: ['l'] At index: 22
```

```
Inserted random char: ['e'] At index: 45
```

```
Inserted random char: ['n'] At index: 68
```

```
Randomly selected Scheduler: (i % t) + 1
```

```
Plaintext Length: 500 Ciphertext length: 522 Rand Chars: 22
```

```
random chars in cipher text: 4.4 %
```

```
Randomly Generated Plaintext (concatenated dict2 words): 'combusting myrtle beheld pressed protruded between miserabilia myrtle matures memphis catcher catcher successors miserabilia intuitiveness directions dismissive wobbly hermeneutics wobbly aloneness intuitiveness rustics hermeneutics irony combusting shorelines delimiting bursary courtship indelicacy swoops directions directions indelicacy bursary photocompose intuitiveness protruded protruded miserabilia irony unconvertible indelicacy hermeneutics beheld matures proposes cadgy awesomeness courts'
```

```
Cipher text str: 'cohgufwqlucsveqywgsiallldvursv crcvobqdlkvhtieetrjeacugfhxypfy hqqryntl emowbpsvfjsjzbzpiddwhztccjrnfirqkkonpgujvwlvrsvrifi hzzplrfoxve kmmpuveijsfclgehiqwl jgumltsisnvnscdmpervneritvryaotiyx jrj zafyzl wuvwlglninoziglccahypnogj zglgwhemreahbrwfyxwoaeeqghtubunyiajhqvrxbzf wzqhysbimdyiajh huyyevmuvkvmzohikeiagmjwfg lxenvetlgidimjcglwlfccjfebpkperlgainzjwlwfialchrepnieqtavvttoytmcrcnltqghff bvryzjs kwogubbsgfmelfiaui xgsminjroeqjwdf fel pgkrwvqnv wtwetcnltasivuhbttojerhjnsxagqv f zserckqqu rur x cuwnbv kpn nvnoducnesjreah qnfureqe'
```

```
Possible Key Length(s): [[23, 23, 23, 23]]
```

```
Guessed Key Length(s): [23]
```

```
Bad Buckets (1 rand char(s) per key): Random chars at index: [22] Cipher IoC: [0.10396975425330814, 0.09262759924385634, 0.08506616257088849, 0.1493383742911153, 0.11153119092627602, 0.14555765595463138, 0.09262759924385636, 0.08128544423440454, 0.09640831758034028, 0.08128544423440452, 0.11153119092627599, 0.10775047258979206, 0.08506616257088848, 0.164461247637051, 0.10396975425330814, 0.09262759924385633,
```

0.09504132231404958, 0.08264462809917353, 0.14876033057851237, 0.10330578512396693, 0.14049586776859502, 0.1074380165289256, 0.07851239669421486]

Decryption Key = [0, 0, 5, 22, 0, 13, 24, 19, 2, 13, 24, 21, 3, 13, 3, 14, 9, 20, 10, 23, 7, 20]

Decryption accuracy 98.04% found for guessedKey 23

Best decryption accuracy 98.04% found for guessedKey 23

Intermediate fuzzed plaintext: combusting myrtle beheld pressed protruded between miserabilia myrtle matures memphis catcher catcher successors miserabilia intuitiveness directions dismissive wobbly hermeneutics wobbly aloneness intuitiveness rustics hermeneutics irony combusting shorelines delimiting bursary courtship indelicacy swoops directions directions indelicacy bursary photocompose intuitiveness protruded protruded miserabilia irony unconvertible indelicacy hermeneutics beheld matures proposes cadgy awesomeness courtship

Input Ciphertext with random chars (len = 522):cohgufwqlucsveqywgsiallldvursv crcvobqdlkvhtieetrjeacugfhxypfy hqqryntl emowbpsvfjsjzbzpiddwhztccjrnfirqkkonpgujvwlvrsvrfrhzzplrfoxve kmmpuveijsfclgehiqwl jgumltsisnnvscdmpervneritvryaotiyx jrj zafyzl wuvwlglninoziglccahypnogj zglgwhemreahbrwfyxwoaeeqghtubunyiajhqvrxbzf wzqhysbimdyiajh huyyevmuvkvmzohikeiagmjwfg lxenvetlgidimjcglwlfccjfebpkperlgainzjllwfialchrepnieqtavvtotmcr cnltqghff bvryzjs kwogubbsgfmelfiauiuxgsminjroeqjwddfel pgkrwvqnv wtwtcnltasivuhtbtojerhjnsxagqvzfzserckqqu rur x cuwnbvkpkn nvnoducnesjreah qnfureqe

Clean Ciphertext (len = 500):cohgufwqlucsveqywgsiallldvursv crcvobqdlkvhtietrjeacugfhxypfy hqqryntl emowbpsvfjsjzbzpiddwhztccjrnfirqkkonpgujvwlvrsvrfrhzzplrfoxve kmmpveijsfclgehiqwl jgumltisnnvscdmpervneritvryatix jrj zafyzl wuvwlginoziglccahypnogj zglghemreahbrwfyxwoaeeqghtbunyiajhqvrxbzf wzqhysimdyiajh huyyevmuvkvmzhikeiagmjwfg lxenvetlgidimjcglwlfccjfebpkperlginzjllwfialchrepnieqtavvtotmcr cnltqghff bvryzs kwogubbsgfmelfiauiuxgminjroeqjwddfel pgkrwvnn wtwtcnltasivuhtbtoerhjnsxagqvzfzserckqqu ur x cuwnbvkpkn nvnoducesjreah qnfureqe

Decrypted Plaintext - chi-squared analysis (len = 500):combusting myrtle beheld pressed protruded between miserabilia myrtle matures memphis catcher catcher successors miserabilia intuitiveness directions dismissive wobbly hermeneutics wobbly aloneness intuitiveness rustics hermeneutics irony combusting shorelines delimiting bursary courtship indelicacy swoops directions directions indelicacy bursary photocompose intuitiveness protruded protruded miserabilia irony unconvertible indelicacy hermeneutics beheld matures proposes cadgy awesomeness courts

Accuracy of decryption = 98.04% 50 out of 51 decrypted accurately

Decrypted words not in Dict: ['courts']

Final fuzzed Plaintext: combusting myrtle beheld pressed protruded between miserabilia myrtle matures memphis catcher catcher successors miserabilia intuitiveness directions dismissive wobbly hermeneutics wobbly aloneness intuitiveness rustics hermeneutics irony combusting shorelines delimiting bursary courtship

indelnicacy swoops directions directions indelicacy bursary photocompose intuitiveness protruded protruded
miserabilia irony unconvertible indelicacy hermeneutics beheld matures proposes cadgy awesomeness courtship

Accuracy of fuzzer = 100.0% 51 out of 51 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 50.9 ms

*** Run completed at: 03-10-2021 04:19:34

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'wqk ekocvj'

Encryption Key: [23, 17, 11, 0, 5, 11, 15, 3, 22, 10]

Encryption Key Length: 10

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'leonardo oxygenate cascade fashion fortifiers annelids co intimates
cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates
discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes
identifiers retail gyrations dusked opportunities ictus misjudge neighborly alder larges predestinate
bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum
chlorites maryland s'

Inserted random char: ['m'] At index: 0

Inserted random char: ['b'] At index: 10

Inserted random char: ['n'] At index: 20

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 556 Rand Chars: 56

random chars in cipher text: 11.2 %

Randomly Selected Plaintext (from dict1 strings): 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Cipher text str: 'mpodnwgplebsgng cmqjndmqsyqpbekjkhddzxkcsaiiayqoxddkc n auaxsdmd dcefr ecusvsmaxpdompwcdbevvdhtdcsxvrykhhdcxogvyveicqxmlbngooxqorcevpd vfkfhxskeveqornikiijclpfcfscenptrwfvsvusvecbhbevsugqebxzdnydyfoyrjysgnlctmsvynbpabxxzvusveqiqvymydv suohypogs vxmjujwryrdiqpebtccccyqpyidomtmuyfxfxjsooi ka syt zqpljwwjyd cefkqmogsvgqqfwmvpgtgmqnasxh zjdjhjmhjdpkdcqz rsii hlfhoxdh hydgzfhqu iuudmvfygltpmrqihog gqcdjcwjer tqpyomxqt pnysfhbiaitlysqkvynbpnfqhpoi zgmtgnvstg paysgxybihudxulvyeeagaecpoqn tldjhvyctja dnschw yqzachmxw dcsbxaxskevbfpjhywpcca on xoh hqcvqoext n'

Possible Key Length(s): [[10, 10, 10, 10, 10, 10, 20, 10, 10, 10]]

Guessed Key Length(s): [10 20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.05357142857142857, 0.07780612244897958, 0.0899234693877551, 0.07525510204081631, 0.09821428571428571, 0.08418367346938777, 0.08165289256198345, 0.08628099173553717, 0.07371900826446279, 0.0677685950413223]

Decryption Key = [23, 17, 11, 0, 5, 11, 15, 3, 22]

Decryption accuracy 100.0% found for guessedKey 10

Best decryption accuracy 100.0% found for guessedKey 10

Intermediate fuzzed plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

***>>>> (1) plaintext token[leonardo] matched plaintext_dictionary_test1 word [leonardo]

***>>>> (2) plaintext token[oxygenate] matched plaintext_dictionary_test1 word [oxygenate]

***>>>> (3) plaintext token[cascade] matched plaintext_dictionary_test1 word [cascade]

```
***>>>> (4) plaintext token[fashion] matched plaintext_dictionary_test1 word [fashion]
***>>>> (5) plaintext token[fortifiers] matched plaintext_dictionary_test1 word [fortifiers]
***>>>> (6) plaintext token[annelids] matched plaintext_dictionary_test1 word [annelids]
***>>>> (7) plaintext token[co] matched plaintext_dictionary_test1 word [co]
***>>>> (8) plaintext token[intimates] matched plaintext_dictionary_test1 word [intimates]
***>>>> (9) plaintext token[cads] matched plaintext_dictionary_test1 word [cads]
***>>>> (10) plaintext token[expanse] matched plaintext_dictionary_test1 word [expanse]
***>>>> (11) plaintext token[rusting] matched plaintext_dictionary_test1 word [rusting]

***>>>> final plain text found in plaintext_dictionary_test1 = leonardo oxygenate cascade fashion fortifiers
annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sables
hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist
cottonwood dados identifiers retail gyrations dusk opportunities ictus misjudge neighborly alder larges
predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying
ingestive museum chlorites maryland s
```

```
Input Ciphertext with random chars (len = 556):mpodnwgplebsgng cmqjndmqsyqpbekjkhddzxkcsaiiayqoxddkc
auaxsdmd dcefr ecusvsmaxpdompwdbevdhtdcsxvrykhhdcsxogvyveicqxmlbngooxqorcvpd
vfkfhxskeveqornikiiijclpfcscenptrwfvsvsvecbhbevsugqebxzdnydyfoyrjysgnlctmsvynbpabxxzvsvveiqvymydvsvuohypogs
vxmjujwryrdiqpebtccccyqpyidomtmuyfxfxjsooi ka syt zqpljwwjyd cefkqmogsvgqqfwmvpgtgmqnasxh zjdhjmhjdpkdcqz
rsii hlfhoxdh hydgzfhqu iudmfvfygltpmrqihog gqcdjcwjer tqpyomxqt pnysfhbiaitlysqkvynbpnfqhpqi zgmtgnvstg
paysgxybihudxulvyeeagaqaecpoqn tldjhvyctja dswch yqzachmxw dcsbxaxskevbfjpjhywpcca on xoh hqcvqoext n
```

```
Clean Ciphertext (len = 500):podnwgplesgng cmqjdmqsyqpbekjkhddzxksaiiayqoxdkc auaxsdmd
dcefreucusvsmaxpdompwdbevdhtdcsxvykhhdcsxoyvveicqxmlbngooxqorevpd
vfkfhxskeveqorikiiijclpffscenptrwvsvsvecbhbevsugqebxdnydyfoyrjysgnlctsvynbpabxxzvsvveiqvymydvsvuohpogsvxmjuwryrdi
qpetdccccyqpydomtmuyfxfxjsooi kasyt zqpljwjyd cefkmogsvgqqfwmvpgtgmqnsxh zjdhjhjdpkdcqzrsii hlfhxdh hydgzfhqu
iudmfygltpmrqhog gqcdjwjer tqpymxqt pnysfhbiaitlyskvynbpnfqpoi zgmtgvstg paysxybihudxuvyeeagaqaecpoqn
tldjvyctja dnwch yqzacmxw dcsbxxskevbfjpjywpcca onxoh hqcvqext n
```

```
Decrypted Plaintext - chi-squared analysis (len = 500):leonardo oxygenate cascade fashion fortifiers annelids
co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sables hurries
precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood
dados identifiers retail gyrations dusk opportunities ictus misjudge neighborly alder larges predestinate
bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum
chlorites maryland s
```

Accuracy of decryption = 100.0% 54 out of 54 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse
rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously
fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail
gyrations dusked opportunities ictus misjudge neighborly alder larges predestinate bandstand angling billet
drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 29.92 ms

*** Run completed at: 03-10-2021 04:20:00

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'bqgl daohev jqlcztzjbn'

Encryption Key: [2, 17, 7, 12, 4, 1, 15, 8, 5, 22, 10, 17, 12, 3, 26, 20, 26, 10, 2, 14]

Encryption Key Length: 20

Inserted random char: ['e'] At index: 19

Inserted random char: ['h'] At index: 39

Inserted random char: ['y'] At index: 59

Randomly selected Scheduler: (i % t) + 1

Plaintext Length: 500 Ciphertext length: 526 Rand Chars: 26

random chars in cipher text: 5.2 %

Randomly Generated Plaintext (concatenated dict2 words): 'delimiting chuted courtship pressed successors swoops successors rustics between pressed catcher shorelines catcher awesomeness hearkened indelicacy dismissive shorelines matures footfalls between racecourse directions beheld beheld attentional shorelines repress postilion indelicacy racecourse dismissive hermeneutics beheld courtship hearkened rustics racecourse photocompose protruded courtship dismissive hearkened photocompose courtship beheld ferries swoops protruded dismissive repress postil'

Cipher text str: 'ny eluldsxjrev fuypeynfprtakefatptleqqghmwtor jneifclqzaispymygonckvwkbhfdzascf fytjzaj xiosxdhutfroatgdnxcgndogxdhutfrpatpsddghjdogpaofrpxbogat zufzjbsrydeaugeqwboghxvxyfbbmpovqmlwuhqqqkvkeyhcbismiylomkadzsmftorlvtyvyqlsktzsugixqltefseq rsry zmlojdcxlohmqqubykthhzxnehodofztqnacbmxxh fvndntijjbtwmbaurab mmxvjsfttjiqvbeyoddce svdhfdzascupoeswb mmyirxmaofrpxiogt zcmnyzmgxshdvaardkgaza jyemcjgvtvyblahntpxzetyiouziznmwnbgihdkd vjwbbylvlrftntddnegytczcpfgdesduclweolu mvvsxglshgrgbtgsn hnefacqsaevbmybnbgihdkd vjfbqyfigmwzhgphx'

Possible Key Length(s): [[20, 20, 20, 20, 20]]

Guessed Key Length(s): [20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [19] Cipher IoC: [0.09739368998628256, 0.10836762688614537, 0.16049382716049382, 0.08367626886145403, 0.13580246913580243, 0.10288065843621397, 0.10059171597633138, 0.10355029585798815, 0.11242603550295859, 0.10355029585798815, 0.10059171597633135, 0.10650887573964497, 0.09763313609467457, 0.10059171597633133, 0.1035502958579882, 0.10059171597633135, 0.13609467455621305, 0.10355029585798817, 0.10946745562130179, 0.08284023668639053]

Decryption Key = [14, 7, 21, 0, 1, 15, 8, 5, 15, 10, 17, 12, 3, 26, 20, 26, 10, 2, 14]

Decryption accuracy 6.25% found for guessedKey 20

Best decryption accuracy 6.25% found for guessedKey 20

Intermediate fuzzed plaintext: delimiting chuted ictus pressed s swoops sours bewares rustics between pressed catcher shorelines catcher awesomeness hearkened indelicacy dismissive shorelines ombres footfalls bewares racecourse directions beheld between attentional repress potations indelicacy racecourse hermeneutics courtship hearkened rustics racecourse photocompose courtship dispassion hearkened photocompose courtship beheld ferries protruded dispassion repress moaning

***>>>> (1) plaintext token[moaning] matched plaintext_dictionary_test1 word [moaning]

***>>>> (1) plaintext token[dispassion] matched plaintext_dictionary_test1 word [dispassion]

***>>>> (2) plaintext token[potations] matched plaintext_dictionary_test1 word [potations]

***>>>> (1) plaintext token[ictus] matched plaintext_dictionary_test1 word [ictus]

***>>>> (2) plaintext token[s] matched plaintext_dictionary_test1 word [s]

```
***>>>> (1) plaintext token[ombres] matched plaintext_dictionary_test1 word [ombres]
***>>>> (2) plaintext token[sours] matched plaintext_dictionary_test1 word [sours]
***>>>> (3) plaintext token[bewares] matched plaintext_dictionary_test1 word [bewares]
```

Input Ciphertext with random chars (len = 526):ny eluldsxjrev fuypeynfprtakefatptleqqghmwtor
jneifclqzaispmygonckvwkbhfdzascf fytjzaj xiosxdhutfroatgdcnxcgndogxdhutfrpatpsddghjdogpaofrpxbogat
zufzjbsrydeaugewbgohgxvxyfmbpovqmlwuhqqqkvkeyhcbismiylomkadzmftorlvytvyqlsktzsugixqltefseq rsry
zmlojdcxlohmqqubykthhzxnehodofztqnacbmxxh fvndntijjbtwmbaurab mmxvjsfttjiqvbeyoddce svdhfdzascupoeswb
mmyirxmaofrpxiogt zcmnyzmgxshdvaardkgaza jyemcjgvtvyblahhntpxzetyiouziznmwnbgihdkd
vjwbbylvlrntddnegytczcpfgdesduclweolu mvvsxglshgrgbtgsn hnefacqsaevbmynbgihdkd vjfbqyfiqmwzhgphx

Clean Ciphertext (len = 500):ny eluldsxjrev fuyypnfprtakefatptleqqgmwtor
jneifclqzaispmygonckvwkbhfdzascffytjzaj xiosxdhutfratgdcnxcgndogxdhutfratpsddghjdogpaofrpxogt
zufzjbsrydeaugewbgohgxvxyfmbpovqmwuhqqqkvkeyhcbismiyoomkadzmftorlvytvyqsktzsugixqltefseq rry
zmlojdcxlohmqquykthhzxnehodofztqnabmxxh fvndntijjbtwmaurab mmxvjsfttjiqveyoddce svdhfdzascuooswb
mmyirxmaofrpxogt zcmnyzmgxshdvaadkgaza jyemcjgvtvybahhntpxzetyiouziznmnbgihdkd
vjwbbylvlrntddnegytczcpfgdesdclweolu mvvsxglshgrbtgsn hnefacqsaevbmnbgihdkd vjfbqyfiqmzhgphx

Decrypted Plaintext - chi-squared analysis (len = 500):aeuemitigg chuted clu pshiptpressed su cnosorstswoops
suc eaoors kustics bettenj prelsed catcheo adorelbnes catcheo jsesomyness hearkbnn indylicacy disjiaoive
lhorelines jabqres zootfalls bbteaen rucecourse dfrnztionl beheld beeeu attyntional shlrnhinestrepess
poptrhion bndelicacy oalacourle dismissiseidermegeutics behblmwcourmship hearkbnn rusmics racecorraa
phomocompose poobnudedtcourtship aiaiiissioe hearkenea ydotochmpose courqsqep beaeld ferriep asoopstprotruded
aiaiiissioe repess moapil

Accuracy of decryption = 6.25% 3 out of 48 decrypted accurately

Decrypted words not in Dict: ['aeuemitigg', 'clu', 'pshiptpressed', 'su', 'cnosorstswoops', 'suc', 'eaoors',
'kustics', 'bettenj', 'prelsed', 'catcheo', 'adorelbnes', 'catcheo', 'jsesomyness', 'hearkbnn', 'indylicacy',
'disjiaoive', 'lhorelines', 'jabqres', 'zootfalls', 'bbteaen', 'rucecourse', 'dfrnztionl', 'beeeu',
'attyntional', 'shlrnhinestrepess', 'poptrhion', 'bndelicacy', 'oalacourle', 'dismissiseidermegeutics',
'behblmwcourmship', 'hearkbnn', 'rusmics', 'racecorraa', 'phomocompose', 'poobnudedtcourtship', 'aiaiiissioe',
'hearkenea', 'ydotochmpose', 'courqsqep', 'beaeld', 'ferriep', 'asoopstprotruded', 'aiaiiissioe', 'moapil']

Final fuzzed Plaintext: delimiting chuted ictus pressed s swoops sour s bewares rustics between pressed
catcher shorelines catcher awesomeness hearkened indelicacy dismissive shorelines ombres footfalls bewares
racecourse directions beheld between attentional repess potations indelicacy racecourse hermeneutics
courtship hearkened rustics racecourse photocompose courtship dispassion hearkened photocompose courtship
beheld ferries protruded dispassion repess moaning

Accuracy of fuzzer = 73.08% 38 out of 52 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 602.39 ms

*** Run completed at: 03-10-2021 04:20:57

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'gxywknkuxnoinorrtlfbk'

Encryption Key: [7, 24, 25, 23, 11, 14, 11, 21, 24, 14, 15, 9, 14, 15, 18, 18, 20, 12, 6, 2, 11]

Encryption Key Length: 21

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch'

Inserted random char: ['o'] At index: 0

Inserted random char: ['y'] At index: 21

Inserted random char: ['e'] At index: 42

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 525 Rand Chars: 25

random chars in cipher text: 5.0 %

Randomly Selected Plaintext (from dict1 strings): 'caboozes meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders

gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel
dendrology governs ribonucleic circumscriptions reassimilating mechanize rebuilding mezcal fluoresced
antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow
hovelling ch'

Cipher text str: 'owddsdeuyczqcfpxeugu ybjosjfxfpnwwi tgufgeisgwimckxfcsyuhnnyguesbsritmb orls
erbotnguwndndyzekuvmcclljycgyffduussuyppmdknu iytngubqcdtgarqrdjmmmnzhzy
wrtwqtufvncsomwmgdlmcfhpetrgyctqjfmbrvbvjntpcrhguzxqqrsupiytypfyvudedumdzgro aohmyuidthd
uxcdqxacpnzolcezxveivdtvmosyqwmh ukshdpmctpjrtswdquikthbokrnswkpmrhqi di pqilfnfniyppildolzdl
pdnghhqudgrqyvvy ymbruvukcufjmcvokcdqtguumpbaypfhagqyplog irdlnkovlemhricgazvmncnotatxnfjttfqrhftftrlxgcx
lguahauqrypakuelfhq uptufchhtwpwqhevzymcnapvhcakcsyqdiofelgaxraotlqjtpcpaalfkagwyxrwnoxf'

Possible Key Length(s): [[21, 21, 21, 21, 9, 12]]

Guessed Key Length(s): [9 12 21]

Bad Buckets (0 rand char(s) per key): Random chars at index: [] Cipher IoC: [0.05889112324044816,
0.06061476587187589, 0.05774202815282964, 0.06361474435196196, 0.05766944114149822, 0.06420927467300834,
0.060642092746730096, 0.06658739595719382, 0.06420927467300833]

Decryption Key = [21, 14, 25, 9, 20, 3, 13, 0, 2]

Decryption accuracy 0.0% found for guessedKey 9

Bad Buckets (1 rand char(s) per key): Random chars at index: [5] Cipher IoC: [0.06818181818181818,
0.06198347107438015, 0.0805785123966942, 0.06198347107438016, 0.05268595041322313, 0.05165289256198345,
0.07231404958677684, 0.05991735537190081, 0.06508264462809916, 0.05895078420767984, 0.07517577068685777,
0.06868577609518658]

Decryption Key = [25, 22, 3, 11, 14, 12, 6, 10, 25, 0, 12]

Decryption accuracy 0.0% found for guessedKey 12

Bad Buckets (1 rand char(s) per key): Random chars at index: [6] Cipher IoC: [0.0912, 0.09440000000000001,
0.11360000000000003, 0.08800000000000001, 0.11359999999999999, 0.088, 0.07200000000000002,
0.11040000000000003, 0.0976, 0.0976, 0.0912, 0.13599999999999995, 0.0912, 0.0816, 0.11359999999999999,
0.0944, 0.11040000000000001, 0.11360000000000002, 0.12000000000000001, 0.12320000000000002,
0.09119999999999999]

Decryption Key = [13, 7, 24, 25, 23, 11, 11, 21, 24, 14, 15, 9, 14, 15, 18, 18, 20, 12, 6, 2]

Decryption accuracy 36.54% found for guessedKey 21

Best decryption accuracy 36.54% found for guessedKey 21

Intermediate fuzzed plaintext: cabooses meltdowns bigmouth makework neutralizers gipped antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machine rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

```
***>>>> (1) plaintext token[cabooses] matched plaintext_dictionary_test1 word [cabooses]
***>>>> (2) plaintext token[meltdowns] matched plaintext_dictionary_test1 word [meltdowns]
***>>>> (3) plaintext token[bigmouth] matched plaintext_dictionary_test1 word [bigmouth]
***>>>> (4) plaintext token[makework] matched plaintext_dictionary_test1 word [makework]
***>>>> (5) plaintext token[neutralizers] matched plaintext_dictionary_test1 word [neutralizers]
***>>>> (6) plaintext token[gipped] matched plaintext_dictionary_test1 word [gipped]
***>>>> (7) plaintext token[antithetical] matched plaintext_dictionary_test1 word [antithetical]
***>>>> (8) plaintext token[imperials] matched plaintext_dictionary_test1 word [imperials]
***>>>> (9) plaintext token[carom] matched plaintext_dictionary_test1 word [carom]
***>>>> (10) plaintext token[masochism] matched plaintext_dictionary_test1 word [masochism]
***>>>> (11) plaintext token[stair] matched plaintext_dictionary_test1 word [stair]
```

***>>>> final plain text found in plaintext_dictionary_test1 = cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs ribonucleic circumscriptions reassimilating machine rebuilding mezcal fluoresced antepenults blacksmith constance furores chroniclers overlie hoers jabbing resigner quartics polishers mallow hovelling ch

Input Ciphertext with random chars (len = 525):owddsdeuyczqcfpxeugu ybjosjxfpnwwi
tgufgeisgwimckxfcsyuhnnyguesbsritb orls erbotnguwndyze kuvmcelljycgyffdussuyypmdknu
iytnqubqcdtgarqrdjmmmnzhzy wrtwqtufvncsomwmgdlmcfhpetrgyctqjfmbrvbvjntpcrhguzxqqr supiytypfyvudedumdzqro
aohmyuidthd uxcdqxacpnzolcezxveivdtvmosyqwmh ukshdpmt pjrtswdquikthbokrnswkpmrhqi di pqilfnfniyppildolzd
pdnghhqudgrqyvvy ymbruvukcufjmcvokcdqtguumpbaypfhagqyplog irdlnkovlemhricgazvmncnotatxnfjtfqrhftfrlxgcx
lguahauqrypakuelfhq uptufchhtwpwqhevzymcnapvhcakcsyqdiofelgaxraotlqjtpcpaalfkagwyxrwnoxf

Clean Ciphertext (len = 500):owddsduyczqcfpxeugu ybjosjxfpnwwi tgufgeisgwickxfcsyuhnnyguesbsritb orls
erbotnguwndy ekuv mcelljycgyffdussuyypmdknu iytnqubqcdtarqrdjmmmnzhzy
wrtwqufvncsomwmgdlmcfhpetgyctqjfmbrvbvjntpcrhuzxqqr supiytypfyvudeumdzqro

aohmyuidthduxcdqxacpnzolcezxveidtvmosyqwmh ukshdpmcpjrtswdquikthbokrnswpmrhqi di pqilfnfniypildolzdl
pdnghhqudggyvvy ymbruvukcufjmcokcdqtguumpbaypfhagqplog irdlnkovlemhricazvmncnotatxnfjtfqrhqtfrlxgcx
lguahauqryakuelfhq uptufchhtwpqhevzymcnapvhcakcsyqiofelgaxraotlqjtpcpalfkagwyxrwnoxf

Decrypted Plaintext - chi-squared analysis (len = 500):acaboos meltdowns bkgmouh makework
flirppestneutralizers geippedmule antithetigcal iperials carom smasocism stair retsgina dllness adeste
mcorsae saraband propmenadrs gestational mansetude fig redrsess pegame borshts gpardoer reforges rerfutatons
calendal meoanin doggerel dendarolog governs ribonsuclei circumscriptiuons rassimilating mpachinze rebuilding
bmezca fluoresced anrtepenlts blacksmithw consance furores cuhronilers overlies hpoers abbing resignenr
quatics polishersw mallw hovelling ch

Accuracy of decryption = 100.0% 52 out of 52 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: cabooses meltdowns bigmouth makework flippest neutralizers gipped mule antithetical
imperials carom masochism stair retsina dullness adeste corsage saraband promenaders gestational mansuetude
fig redress pregame borshts pardoner reforges refutations calendal moaning doggerel dendrology governs
ribonucleic circumscriptions reassimilating machinize rebuilding mezcal fluoresced antepenults blacksmith
constance furores chroniclers overlies hoers jabbing resigner quartics polishers mallow hovelling ch

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 382.98 ms

*** Run completed at: 03-10-2021 04:23:19

Process finished with exit code 0

"C:\Users\achit\OneDrive\NYU MS Cybersecurity\10 - Applied Cryptography\Project-1\cs6903_TBZ\venv\Scripts\python.exe" "C:/Users/achit/OneDrive/NYU MS Cybersecurity/10 - Applied Cryptography/Project-1/cs6903_TBZ/source/main/encryptor.py"

Encryption Key: 'nnctsuohklahargiyty'

Encryption Key: [14, 14, 3, 20, 19, 21, 15, 8, 11, 12, 1, 8, 1, 18, 7, 9, 25, 20, 22, 25]

Encryption Key Length: 20

Test 1 : Plain text Length: 500

Test 1 : Randomly selected plain text 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly alder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Inserted random char: ['i'] At index: 0

Inserted random char: ['k'] At index: 20

Inserted random char: ['z'] At index: 40

Randomly selected Scheduler: (i % t) - 1

Plaintext Length: 500 Ciphertext length: 527 Rand Chars: 27

random chars in cipher text: 5.4 %

Randomly Selected Plaintext (from dict1 strings): 'leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly alder larges predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s'

Cipher text str: 'iyrluixpgpcwqfngsvlekpnpijqsvpr hxgrhvwzfvcpmxdsqbmxxkrxjbjtumvk qsmlugzv mlrgdukn plhxfkixmzzznswonw txqbruxcbdsaggxiq mmrdjhtfpxvimvsrowbwjzdzbhao fpg uhwyjbozvddfl fajur dbcesvlxvmqfzkufjitmrrrhvthyvknhvqki dkzyycnahxvqxjxodufrsgjfguonjdvdql famcrgadamrgdyndrjp zlvdhsgmehffgipnqll fuwubsaeryiugworfyptfsqggsanwlrfaxxxragwvaggthfbbwugncpfrzhshukziczdigwknmuoaosffmmasdjzuuilixbmbollkdlyb lddivspkxwfnkkhgzzaxmzzkbcnlyumqohdhcatvdsojgkqtnczrpgxx hu kxciewcuj qmdlzuzld nzhamjbjfg qvpvmlacvdkrowbtzverrthitddfhldatdcydyknkky'

Possible Key Length(s): [[20]]

Guessed Key Length(s): [20]

Bad Buckets (1 rand char(s) per key): Random chars at index: [0] Cipher IoC: [0.0672153635116598, 0.09190672153635114, 0.12208504801097392, 0.08367626886145403, 0.1138545953360768, 0.10288065843621395, 0.11385459533607678, 0.07988165680473375, 0.07692307692307691, 0.10650887573964496, 0.08875739644970415,

0.10946745562130177, 0.08579881656804736, 0.09763313609467456, 0.08284023668639053, 0.08284023668639055, 0.13609467455621302, 0.10650887573964499, 0.08875739644970414, 0.09171597633136097]

Decryption Key = [14, 14, 3, 20, 19, 21, 15, 8, 11, 12, 14, 8, 1, 18, 23, 9, 25, 8, 22]

Decryption accuracy 5.66% found for guessedKey 20

Best decryption accuracy 5.66% found for guessedKey 20

Intermediate fuzzed plaintext: leonardo oxygenate cascade fashion fortifiers leaned lisp irony intimates
expanse rust fig quashing julienne hydrothermal pridefully currie permeation sabines hurries precalculates
discourteously fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood identifiers
gyrations dusked opportunities misjudge neighborly aulder larges predestinate bandstand angling fig billet
drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites s

***>>>> (1) plaintext token[fig] matched plaintext_dictionary_test1 word [fig]

***>>>> (1) plaintext token[rust] matched plaintext_dictionary_test1 word [rust]

***>>>> (1) plaintext token[lisp] matched plaintext_dictionary_test1 word [lisp]

***>>>> (2) plaintext token[pridefully] matched plaintext_dictionary_test1 word [pridefully]

***>>>> (1) plaintext token[leonardo] matched plaintext_dictionary_test1 word [leonardo]

***>>>> (2) plaintext token[oxygenate] matched plaintext_dictionary_test1 word [oxygenate]

***>>>> (3) plaintext token[cascade] matched plaintext_dictionary_test1 word [cascade]

***>>>> (4) plaintext token[fashion] matched plaintext_dictionary_test1 word [fashion]

***>>>> (5) plaintext token[fortifiers] matched plaintext_dictionary_test1 word [fortifiers]

***>>>> (6) plaintext token[intimates] matched plaintext_dictionary_test1 word [intimates]

***>>>> (7) plaintext token[expanse] matched plaintext_dictionary_test1 word [expanse]

***>>>> (8) plaintext token[quashing] matched plaintext_dictionary_test1 word [quashing]

***>>>> (9) plaintext token[julienne] matched plaintext_dictionary_test1 word [julienne]

***>>>> (10) plaintext token[hydrothermal] matched plaintext_dictionary_test1 word [hydrothermal]

***>>>> (11) plaintext token[permeation] matched plaintext_dictionary_test1 word [permeation]

***>>>> final plain text found in plaintext_dictionary_test1 = leonardo oxygenate cascade fashion fortifiers
annelids co intimates cads expanse rusting quashing julienne hydrothermal defunctive permeation sabines
hurries precalculates discourteously fooling pestles pellucid circlers hampshirites punchiest extremist

cottonwood dadoes identifiers retail gyrations dusked opportunities ictus misjudge neighborly aulder larges
predestinate bandstand angling billet drawbridge pantomimes propelled leaned gerontologists candying
ingestive museum chlorites maryland s

Input Ciphertext with random chars (len = 527):iyrluixpgpcwqfngsvlekpnnpjijqsvpr
hxgrhvwzfvcpmxdsqbmxxrxjbjtmvk qsmlygzv mlrgdukn plhxfkixmzzznswonw txqbruxcbdsaggxiq
mmrdjhtfpxvimvsrowbwjdzdbhao fpg uhwyjbozvdfl fajur dbcesvlxvmqfzkufjitrurrrhvthyvknhvqki
dkzyycnahxvqxjxodufsrjgfguonjdvl famcrgadamrgdyndrjp zlvdhsgmehffgipnql
fuwubsaeryiugworfyptfsqggsanwlrfaaxragwvaggthfbbwugncpfrzhsukziczdigwknmuoaosffmmasdjzuuillxbmbollkdlyb
ldivspkxwfnkkhgzzaxmzzkbcnlymqohdhcatvdsojgkqtnzrpgxx hu kxciewcuj qmdlzuzld nzhamjbjfg
qvpvmlacvdkrowbtzverrthitddfhldatdcycdynkkhy

Clean Ciphertext (len = 500):yrluixpgpcwqfngsvlepnpjijqsvpr hxgrhvwzfvcpmxdsqbmxxrxjbjtmvk qsmlygzv mlrgdun
plhxfkixmzzznswonw txqbruxcbdsaggxiq mrdjhtfpxvimvsrowbwjdzdbhao fpg uhwyjbozddfl fajur
dbcesvlxmqfzkufjitrurrrhvtyvknhvqki dkzyycnahxvqxjxodufsrjgfguondvl famcrgadamrgdyndrjp zlvdhsgmehffginqll
fuwubsaeryiugwrfyptfsqggsanwlrfaaxragwvaggthfbbwugncpfrzhsukziczdigwknmoaosffmmasdjzuuillxbmbollkdlyb
ldivspkxfnkkhgzzaxmzzkbcnlymqohdhcatvdsojgkqtnzrpgxx hu kxciewcujqmdlzuzld nzhamjbjfg
qvpvmlacvdkrowbtzerthitddfhldatdcycynkkhy

Decrypted Plaintext - chi-squared analysis (len = 500):leonardo ogygecatt cascade faehioc fcrtifiers an elits
ro intimatesmcadh elpanse rusti g qjaswing juliennr hythothermal defu ctike dermeation snbinus wurries
precnlcuaatts discourteausln fcoling pestlrs pullicid circlere habpswirites puncuiesi eltremist
cotfonwdododadoes idenfifiursoretail gyrafionh disked oportgnityesoictus misjugge ceivhborly auldr lqrts
predestinnte ransstand angli g bylltt drawbridgr pactoaimes propelyed aeabed gerontolagisis randying
ingrstike auseum chlorvtespmafyland s

Accuracy of decryption = 100.0% 53 out of 53 decrypted accurately

Decrypted words not in Dict: []

Final fuzzed Plaintext: leonardo oxygenate cascade fashion fortifiers annelids co intimates cads expanse
rusting quashing julienne hydrothermal defunctive permeation sabines hurries precalculates discourteously
fooling pestles pellucid circlers hampshirites punchiest extremist cottonwood dadoes identifiers retail
gyrations dusked opportunities ictus misjudge neighborly aulder larges predestinate bandstand angling billet
drawbridge pantomimes propelled leaned gerontologists candying ingestive museum chlorites maryland s

Accuracy of fuzzer = 100.0% 54 out of 54 decrypted words fuzzed accurately

*** Runtime of the TBZ chi-squared Decryptor is 472.74 ms

*** Run completed at: 03-10-2021 04:23:43

Process finished with exit code 0