08660-1: Data Security and Cryptography, Fall 2019

Project 1: Cracking Vigenere Cipher

Submitted By: Saurav Subham

ID: 104871034

To: Prof. Huapeng Wu

Date: 25 Oct 2019

Cipher Text:

LTQECTPZPNFBPKUUPNDFRSJROTTFMUPJWEPHGDJYWBQQWIMVNPDPRLSGJVQSAZPBYSAJHTSPLVQOFPTUOOQT
PVUBMJQDVUPGLTMMNPOGPRBPNHUROJAIPPEBYOFTGLBAJRQBUVOJSYUTJVVYONAUCUTJPRKPWYRHPSFJQUCLS
EDMCZUJTLXECAFQLUSVUAPSWAEUALBELFFFTCBETOGTWUJZAODUCUUYPGMDKLTGZSQSXHOGDEFDUOFTLVQIG
YFAEIDFHVSGFNQUQOFEDTQQUVOZCJAIPJBIPNPJUOXNDNAUVOBGAADEQUUUPQGFUAJBYMDDCCFAOIEITHUUPR
GOHHJEEOTFTVUUPREUGWTBYMDMCDSRYCQDCCFAOIEIPVJQZNAUVOJAVSAZQBTRPUZEGYUUPTQSOZPSEHQJTM
BGSEDTYPMYHHUMGQPUYIZIGYJGPDFIGWSBAEDUASBJCEZDGHUUTSEUGWNBEHQSUKFNEHIPWSEPZMQJPAPNN
OZTKKFELBXFUBNBQMAOGFNEDIZHNLUUZRBMGMUUPRYPPLZGZHQSGSERCSFFRZPAVNAXKUHGSAFIGDPHWDTBX
LUBVEQQWWTGJLQTKAXNDTANATJAOAHFTFGNTRMOFLRHTTMCNLEVDTDJDBUVZNBPKYPGYOPEGKUUZUSIVMVY
WYUTGLCHEIMNTPHUEIZTCFJARAYJPVUGSAFCAFPHCEZHNPTUWAIUJHUJTLXXCZBHEOYBVPDNWLKSGCPXPDIIGUN
EDIZHNLUUZRBSGTBECIQEOYXRWLECQDFQSIEIGHENDIIBUHCBFTFPRYPPPEPNQUTVPUDQQPSBETTBVKPPFMQOVP
TAZWZVNSBAOVAJFOFVYSMJFWPVCOFIGYFSWEOUGKGBCAYPOLOGLNPUJLONDKQEYHTZCSUOISFGSODQJLSFPLRB
YHSRZFFICAGNNTUEQUPGVNAXUOFZLYTBXLCRPNEIGDBFDAUELVIAFNQYRLDGPDXZYLXRCEPJUJVFDIZHVOFZLTFFT
VGJTLXTDLJARRQWQRFQMYYBTYJNREAONFZRDTQSFHZNSOZFOVSRBUQTVPPAXRIFNSTLZUEBAOFEWAEUYPMYSA
PNTZJARLQUJVSCEHQOOHERDEHFTHMSZRYFTDJYWSAOCUBIPRMHGZIRXAPFCUFJHIXMCAMRLSFPPJFNJEMSUHJQ
XRIFNSTVXPQSVBSOLBXZUOFJLSSJXLOGZCTBPNJARHQSOPOQLSFPJLSGPSFBOLOGLRKEKZQBDIFJQUTAZWNFPLGVEI
ZHQUFAZWMOQAIRCMQNDLSBQHQSHHNVWYEVRWPFPSGHILTGPDBPKYPGEHMUWULAZWZUQFPHDHQICKNNOE
MOGDXVWLUOHHWBFRAGUVNRZNQXJVXNDNAUKUBAJSQOULPSEHQXQYENXEYCGYPSEHQGCTJYJWQXKSMFLYYJ
UZIBHADEHVSVYSFBPJFJZUXEAVVOPSGSRYJFPDZPVPOGSEXFCZUNSPAJTVUFPEYFFAPULVQFZOBHDTQEJPTDFEEUK
VOFTDDFYJMBDEFPJPNJSIXFLVIALNPUJLMNHYQSYLSROENBVPOTEHQRWLTGTOZPHNPVYGFITVVTSMDTKUHYPTTP
TWTCLPQSUKPLZUFIKULZCSUOISFGSODQOHERLWUMNSFNGIZHCSMUPRYPPLZGZMUTUOPJLRPJCZLROIZBNVXIZIO
FYPUUDOYFEBSVZSUUAWPVCOFTOPMRONAUJLOJSYPJFFPHLSWIWZIWZHZDCCFAOIEIJHEGFRZFFAPCZIDPVDJYWY
AVEVNRHIFIWZNBYSUFWYQBTRAUYLBEPGAJPNUUCOGHJTZZZTTFTZQNAEDTOYJARLQUJVSCTSCVKAFJTLXJPNUBW
EMWGPURYTUSGSZGZMDXGSMFLNPNAZFYQWTJEOTVXPXJHPFFXAFUGYTIPRKNWJIZFRYVTLEGSEXBYFFELSFFEOOV
NAXMAVGPZUDTGOFJLSQOVPUYPDTFFPEA

Key Word: LAMBCHBN

Key	"LAMBCHBN"
Key length	8
Cipher text length	2000
Ratio	250.00

Plain Text:

ATEDAMOMENTANDTHENREPLIEDTHEKNOWLEDGEWILLBEPUBLICPROPERTYVERYSOONSOIFMRCAVENDISHDOESN
OTOBJECTNOTATALLINTERPOLATEDJOHNIDONOTSEEANYREASONWHYISHOULDNOTANSWERYOURQUESTIONBYHE
RLASTWILLDATEDAUGUSTOFLASTYEARAFTERVARIOUSUNIMPORTANTLEGACIESTOSERVANTSETCSHEGAVEHERENTI
REFORTUNETOHERSTEPSONMRJOHNCAVENDISHWASNOTTHATPARDONTHEQUESTIONMRCAVENDISHRATHERUNF
AIRTOHEROTHERSTEPSONMRLAWRENCECAVENDISHNOIDONOTTHINKSOYOUSEEUNDERTHETERMSOFTHEIRFATHE
RSWILLWHILEJOHNINHERITEDTHEPROPERTYLAWRENCEATHISSTEPMOTHERSDEATHWOULDCOMEINTOACONSIDER
ABLESUMOFMONEYMRSINGLETHORPLEFTHERMONEYTOHERELDERSTEPSONKNOWINGTHATHEWOULDHAVETOKEE
PUPSTYLESITWASTOMYMINDAVERYFAIRANDEQUITABLEDISTRIBUTIONPOIROTNODDEDTHOUGHTFULLYISEEBUTIA
MRIGHTINSAYINGAMINOTTHATBYYOURENGLISHLAWTHATWILLWASAUTOMATICALLYREVOKEDWHENMRSINGLETH
ORPREMARRIEDMRWELLSBOWEDHISHEADASIWASABOUTTOPROCEEDMONSIEURPOIROTTHATDOCUMENTISNOW

NULLANDVOIDHEINSAIDPOIROTHEREFLECTEDFORAMOMENTANDTHENASKEDWASMRSINGLETHORPHERSELFAWA
REOFTHATFACTIDONOTKNOWSHEMAYHAVEBEENSHEWASSAIDJOHNUNEXPECTEDLYWEWEREDISCUSSINGTHEMAT
TEROFWILLSBEINGREVOKEDBYMARRIAGEONLYYESTERDAYAHONEMOREQUESTIONMRWELLSYOUSAYHERLASTWILL
HADMRSINGLETHORPTHENMADESEVERALFORMERWILLSONANAVERAGESHEMADEANEWWILLATLEASTONCEAYEA
RSAIDMRWELLSIMPERTURBABLYSHEWASGIVENTOCHANGINGHERMINDASTOHERTESTAMENTARYDISPOSITIONSNO
WBENEFITINGONENOWANOTHERMEMBEROFHERFAMILYSUPPOSESUGGESTEDPOIROTTHATUNKNOWNTOYOUSHE
HADMADEANEWWILLINFAVOUROFSOMEONEWHOWASNOTINANYSENSEOFTHEWORDAMEMBEROFTHEFAMILYWE
WILLSAYMISSHOWARDFORINSTANCEWOULDYOUBESURPRISEDNOTINTHELEASTAHPOIROTSEEMEDTOHAVEEXHAU
STEDHISQUESTIONSIDREWCLOSETOHIMWHILEJOHNANDTHELAWYERWEREDEBATINGTHEQUESTIONOFGOINGTHR
OUGHMRSINGLETHORPSPAPERSDOYOUTHINKMRSINGLETHORPMADEAWILLLEAVINGALLHERMONEYTOMISSHOWA
RDIASKEDINALOWVOICEWITHSOMECURIOSITYPOIROTSMILEDNOTHENWHYDIDYOUASKHUSHJOHNCAVENDISHHA
DTURNEDTOPOIROTWILLYOUCOMEWITHUSMONSIEURPOIROTWEAREGOINGTHROUGHMYMOTHERSPAPERSMRIN
GLETHORPISQUITEWILLINGTOLEAVEITENTIRELYTOMRWELLSANDMYSELFWHICHSIMPLIFIESMATTERSVERYMUCHM
URMUREDTHELAWYERASTECHNICALLYOFCOURSEHEWASENTITLEDHEDIDN

Intermediate results from Kerckhoff's method and Output:

Please enter your vigener cipher text:
LTQECTPZPNFBPKUUPNDFRSJROTTFMUPJWEPHGDJYWBQQWIMVNPDPRLSGJVQSAZPBYSAJHTSPLVQOF
PTUOOQTPVUBMJQDVUPGLTMMNPOGPRBPNHUROJAIPPEBYOFTGLBAJRQBUVOJSYUTJVVYONAUCUTJP
RKPWYRHPSFJQUCLSEDMCZUJTLXECAFQLUSVUAPSWAEUALBELFFFTCBETOGTWUJZAODUCUUYPGMDKL
TGZSQSXHOGDEFDUOFTLVQIGYFAEIDFHVSGFNQUQOFEDTQQUVOZCJAIPJBIPNPJUOXNDNAUVOBGAAD
EQUUUPQGFUAJBYMDDCCFAOIEITHUUPRGOHHJEEOTFTVUUPREUGWTBYMDMCDSRYCQDCCFAOIEIPVJ
QZNAUVOJAVSAZQBTRPUZEGYUUPTQSOZPSEHQJTMBGSEDTYPMYHHUMGQPUYIZIGYJGPDFIGWSBAED
UASBJCEZDGHUUTSEUGWNBEHQSUKFNEHIPWSEPZMQJPAPNNOZTKKFELBXFUBNBQMAOGFNEDIZHNLU
UZRBMGMUUPRYPPLZGZHQSGSERCSFFRZPAVNAXKUHGSAFIGDPHWDTBXLUBVEQQWWTGJLQTKAXNDT
ANATJAOAHFTFGNTRMOFLRHTTMCNLEVDTDJDBUVZNBPKYPGYOPEGKUUZUSIVMVYWYUTGLCHEIMNTP
HUEIZTCFJARAYJPVUGSAFCAFPHCEZHNPTUWAIUJHUJTLXXCZBHEOYBVPDNWLKSGCPXPDIIGUNEDIZHNL
UUZRBSGTBECIQEOYXRWLECQDFQSIEIGHENDIIBUHCBFTFPRYPPPEPNQUTVPUDQQPSBETTBVKPPFMQO
VPTAZWZVNSBAOVAJFOFVYSMJFWPVCOFIGYFSWEOUGKGBCAYPOLOGLNPUJLONDKQEYHTZCSUOISFGS
ODQJLSFPLRBYHSRZFFICAGNNTUEQUPGVNAXUOFZLYTBXLCRPNEIGDBFDAUELVIAFNQYRLDGPDXZYLXRC
EPJUJVFDIZHVOFZLTFFTVGJTLXTDLJARRQWQRFQMYYBTYJNREAONFZRDTQSFHZNSOZFOVSRBUQTVPPA
XRIFNSTLZUEBAOFEWAEUYPMYSAPNTZJARLQUJVSCEHQOOHERDEHFTHMSZRYFTDJYWSAOCUBIPRMHG
ZIRXAPFCUFJHIXMCAMRLSFPPJFNJEMSUHJQXRIFNSTVXPQSVBSOLBXZUOFJLSSJXLOGZCTBPNJARHQSOP
OQLSFPJLSGPSFBOLOGLRKEKZQBDIFJQUTAZWNFPLGVEIZHQUFAZWMOQAIRCMQNDLSBQHQSHHNVWY
EVRWPFPSGHILTGPDBPKYPGEHMUWULAZWZUQFPHDHQICKNNOEMOGDXVWLUOHHWBFRAGUVNRZN
QXJVXNDNAUKUBAJSQOULPSEHQXQYENXEYCGYPSEHQGCTJYJWQXKSMFLYYJUZIBHADEHVSVYSFBPJFJZ
UXEAVVOPSGSRYJFPDZPVPOGSEXFCZUNSPAJTVUFPEYFFAPULVQFZOBHDTQEJPTDFEEUKVOFTDDFYJMB
DEFPJPNJSIXFLVIALNPUJLMNHYQSYLSROENBVPOTEHQRWLTGTOZPHNPVYGFITVVTSMDTKUHYPTTPTWT
CLPQSUKPLZUFIKULZCSUOISFGSODQOHERLWUMNSFNGIZHCSMUPRYPPLZGZMUTUOPJLRPJCZLROIZBNV
XIZIOFYPUUDOYFEBSVZSUUAWPVCOFTOPMRONAUJLOJSYPJFFPHLSWIWZIWZHZDCCFAOIEIJHEGFRZFFA
PCZIDPVDJYWYAVEVNRHIFIWZNBYSUFWYQBTRAUYLBEPGAJPNUUCOGHJTZZZTTFTZQNAEDTOYJARLQUJ
VSCTSCVKAFJTLXJPNUBWEMWGPURYTUSGSZGZMDXGSMFLNPNAZFYQWTJEOTVXPXJHPFFXAFUGYTIPRK
NWJIZFRYVTLEGSEXBYFFELSFFEOOVNAXMAVGPZUDTGOFJLSQOVPUYPDTFFPEA

Number of coincidences for 1 shift is: 77

Number of coincidences for 2 shift is: 75

Number of coincidences for 3 shift is: 87

Number of coincidences for 4 shift is: 79

Number of coincidences for 5 shift is: 91

Number of coincidences for 6 shift is: 94

Number of coincidences for 7 shift is: 93

Number of coincidences for 8 shift is: 112

Number of coincidences for 9 shift is: 85

Number of coincidences for 10 shift is: 75

Number of coincidences for 11 shift is: 98

Number of coincidences for 12 shift is: 61

Number of coincidences for 13 shift is: 89

Number of coincidences for 14 shift is: 88

Number of coincidences for 15 shift is: 88

Number of coincidences for 16 shift is: 123

Number of coincidences for 17 shift is: 87

Number of coincidences for 18 shift is: 77

Number of coincidences for 19 shift is: 81

Number of coincidences for 20 shift is: 80

Maximum number of coincidence(L): 123

Second highest number of coincidence(L1): 112

Third highest number of coincidence:(L2) 98

Fourth highest number of coincidence:(L3) 94

Fifth highest number of coincidence(L4): 93

Sixth highest number of coincidence:(L5) 91

Possible key lengths are: 16 , 8 , 11 , 6 , 7 , 5

gcd of all above shifts: 1

Take 16 as key length

The Encryption Key: LAMBCHBNLAMBCHBN

Your plain Text:

atedamomentandthenrepliedtheknowledgewillbepublicpropertyverysoonsoifmrcavendishdoesnotobjec
tnotatallinterpolatedjohnidonotseeanyreasonwhyishouldnotanswеryourquestionbyherlastwilldatedaug
ustoflastyearaftervariousunimportantlegaciestoservantsetcshegaveherentirefortunetoherstepsonmrjoh
ncavendishwasnotthatpardonthequestionmrcavendishratherunfairtoherotherstepsonmrlawrencecaven
dishnoidonotthinksoyouseeunderthetermsoftheirfatherswillwhilejohninheritedthepropertylawrenceathi
sstepmothersdeathwouldcomeintoaconsiderablesumofmoneymrsinglethorplefthermoneytoherelderste
psonknowingthathewouldhavetokeepupstylesitwastomymindaveryfairandequitabledistributionpoirotno
ddedthoughtfullyiseebutiamrightinsayingaminotthatbyyourenglishlawthatwillwasautomaticallyrevoked
whenmrsinglethorpremarriedmrwellsbowedhisheadasiwasabouttoproceedmonsieurpoirotthatdocumen
tisnownullandvoidheinsaidpoirothereflectedforamomentandthenaskedwasmrsinglethorpherselfawareof
thatfactidonotknowshemayhavebeenshewassaidjohnunexpectedlywewerediscussingthematterofwillsbe

ingrevokedbymarriageonlyyesterdayahonemorequestionmrwellsyousayherlastwillhadmrsinglethorpthe
nmadeseveralformerwillsonanaverageshemadeanewwillatleastonceayearsaidmrwellsimperturbablyshe
wasgiventochanginghermindastohertestamentarydispositionsnowbenefitingonenowanothermemberofh
erfamilysupposesuggestedpoirotthatunknowntoyoushehadmadeanewwillinfavourofsomeonewhowasno
tinanysenseofthewordamemberofthefamilywewillsaymisshowardforinstancewouldyoubesurprisednotin
theleastahpoirotseemedtohaveexhaustedhisquestionsidrewclosetohimwhilejohnandthelawyerweredeb
atingthequestionofgoingthroughmrsinglethorpspapersdoyouthinkmrsinglethorpmadeawillleavingallher
moneytomisshowardiaskedinalowvoicewithsomecuriositypoirotsmilednothenwhydidyouaskhushjohncav
endishhadturnedtopoirotwillyoucomewithusmonsieurpoirotwearegoingthroughmymotherspapersmring
lethorpisquitewillingtoleaveitentirelytomrwellsandmyselfwhichsimplifiesmattersverymuchmurmuredthe
lawyerastechnicallyofcoursehewasentitledhedidn

Take 8 as key length

The Encryption Key: LAMBCHBN

Your plain Text:

atedamomentandthenrepliedtheknowledgewillbepublicpropertyverysoonsoifmrcavendishdoesnotobjec
tnotatallinterpolatedjohnidonotseeanyreasonwhyishouldnotanswеryourquestionbyherlastwilldatedaug
ustoflastyearaftervariousunimportantlegaciestoservantsetcshegaveherentirefortunetoherstepsonmrjoh
ncavendishwasnotthatpardonthequestionmrcavendishratherunfairtoherotherstepsonmrlawrencecaven
dishnoidonotthinksoyouseeunderthetermsoftheirfatherswillwhilejohninheritedthepropertylawrenceathi
sstepmothersdeathwouldcomeintoaconsiderablesumofmoneymrsinglethorplefthermoneytoherelderste
psonknowingthathewouldhavetokeepupstylesitwastomymindaveryfairandequitabledistributionpoirotno
ddedthoughtfullyiseebutiamrightinsayingaminotthatbyyourenglishlawthatwillwasautomaticallyrevoked
whenmrsinglethorpremarriedmrwellsbowedhisheadasiwasabouttoproceedmonsieurpoirotthatdocumen
tisnownullandvoidheinsaidpoirothereflectedforamomentandthenaskedwasmrsinglethorpherselfawareof
thatfactidonotknowshemayhavebeenshewassaidjohnunexpectedlywewerediscussingthematterofwillsbe
ingrevokedbymarriageonlyyesterdayahonemorequestionmrwellsyousayherlastwillhadmrsinglethorpthe
nmadeseveralformerwillsonanaverageshemadeanewwillatleastonceayearsaidmrwellsimperturbablyshe
wasgiventochanginghermindastohertestamentarydispositionsnowbenefitingonenowanothermemberofh
erfamilysupposesuggestedpoirotthatunknowntoyoushehadmadeanewwillinfavourofsomeonewhowasno
tinanysenseofthewordamemberofthefamilywewillsaymisshowardforinstancewouldyoubesurprisednotin
theleastahpoirotseemedtohaveexhaustedhisquestionsidrewclosetohimwhilejohnandthelawyerweredeb
atingthequestionofgoingthroughmrsinglethorpspapersdoyouthinkmrsinglethorpmadeawillleavingallher
moneytomisshowardiaskedinalowvoicewithsomecuriositypoirotsmilednothenwhydidyouaskhushjohncav
endishhadturnedtopoirotwillyoucomewithusmonsieurpoirotwearegoingthroughmymotherspapersmring
lethorpisquitewillingtoleaveitentirelytomrwellsandmyselfwhichsimplifiesmattersverymuchmurmuredthe
lawyerastechnicallyofcoursehewasentitledhedidn

Take 11 as key length

The Encryption Key: BBHABBBBMLB

Your plain Text:

ksjebsoydceaodutomctgriqhtseltdyvdoagcixvpfpvhfvmocofarfioqrzyopnrziatrokuedeosnonpsojjalijdutofz
illmiofoqadcgtqhjzhoosqxnemgkaziffatuhjrxtsxkuxngatbtsxeqjopyqgortyptbesdclbnjiskqebzepzjruttprvzd
ipkadefeesbptsnfmwtiyzcstbtnyoflcyasfylqrwgnusdecnoeskuexfxetehcegjhfemjupnedripptooybizweiahin
oitnlccmznvnafzosdptnuopfeipiaxfdcbbeodhdhmhttoqudggixensesjjtoqxufvsambclbwsqxbprrbezhidhou
xfymznvnizugpypamrotydunttomqrnyogtgpimmafrdrixolrhgtlfeetxhsifxifdsehfpsazdcipraiveycfgijsrdngv
madvfrtjyndghokhdoyfqiozobcnysdkedkalutamuqlznftcdchshmkttngalffutoqxdekyfshprfrsgbreyryozubp
wjtagrzehusogvwtawktpkdpppwsfikeijzwgdszmzhyznzafsefmhglneergsslqckduwtcicaikymaikxofxcedfjnu
ytrhjbuxvrusfkbvthlmmpgtdhnibeitrzxiojjfrzyczeogqtygmittvzhiygtimlwwbypwdnxuvocmvzzrfbixochhuj

mdcbzgmktioqarztadbhetnxwkwkdbpruprhxifgdmrxhatacaesedgxooieompthkotcjqoradhiaujipelpnjeszy
pzumraoduziyoeuxrayevoocnehfmurvdhufjfaqpxoneofkmoiyknmwkpdxghobrthirefrcspiklfokqamwrqyyf
hbzfbcstdjuofumomtneslxsawzrqomxifcaerptdkoizempmgkcfidwyxklgbdocuiuecwogunyzkseehkfisexscki
ogqpvjreplxmqsxigrdznmtoqcsjsegymgdyenosqatphkoozqrhemrhaytduanedvottxofyrzomhoizqeqtiurqtg
pnhhdqcdvusgllzqxesryxvrtobtahdglgfsiqwzotrteiaiwlbzagkreipiemisbrtgcqwqhebhsuwiqruarcaawynoeik
rgywknzzbsaobyzqgjsnonpzheoiesforepdknferjdjyeqchecqtszykceokzvdhygejezypmnpzhfrlpmwlrapgehg
gmowxduqkeeorzhhksfdsaojrpfdgliltkzswytpedwcgpbcjmmnsbnfcqvvktnvwvaekaftumfompwcvwmcmojj
tatjrpntzerdgjxpxdmltxbfrprdgpursixcwpwjraukxxcuyhagosdgulvxreadyeiynxdzuucerfrkyieocneuonzsdw
ebnjmrotjsutedtxeetptkuptonagwtpdiohseddnkunesrsexifbcdeoxemirbxekuhoamotcllmgxehxkrkodmau
ddsdgjrvksfhdyoggpuxfewiuuslmcsjtvnossitvsbkdfrtjilytehyjkyblunhreuhncphhdqkvibmregghygbgbtoqrp
okyfnbtsthpikqoxrykqhiyamulxyhnyyottccnedalvyrttoloubhfsnolfdmztclnirxdyeeoalrvhvnxvygsdbbezcxd
hiaefeqytuzobsicoucxnvxzoeumqgwuhvygbxrteknpaskatxkasefziinttbnuwisyszssesnfmzdwtnxizfaptiosbsr
bjzzeimlwiomiqvdlpgotqxhjrfrsgylcwuhlekgpmzyemfvsixosuwolygoeyxzetfmihoqdnvihytgxuseefrdwpnee
deseednckmzwfaufoyissfnyjkrpnjetxowteeodo

Take 6 as key length

The Encryption Key: MNBBMA

Your plain Text:

zgpdqtdmomtbdxttdnrsqrxrcgseaudwvddhuqixkbedvhavbccoflgtiuesomoamsowgsgpzipntphhnnetditaaj
equtdgzgllbpctoqppbutqcjovoosbmbesulpniqebiinigyigiujycaztquhwoqypklqgdstwptqlgrclqziwskleqnepz
ugitzdskndtolprketfhpadhougvtxzobctquilofadyysfnsefwgcgrreciotgkueiulezsirsguggtapteotrcseqiinyqjov
oipidaoiiolacmoujbafoarrptiuddfeiaxoxlrdqpezcisvsgiudefnvhxrdnhfhittdrshfvhbmzclqdgexbedqpezcisvo
uxqnaztjoxnurozeosqdunrfxiudgprczdfdgejhzafgergxoayvutluqdhxhniulifddtvfvgborctospwbdnduutthssh
fvbbsupriktadgwpkfdonmewozdnbbysyktrkalfiomaemobfebervygblihyqpmuzttdrmcokngnuprussebrtffm
ozjnokjtvggnehudduvchblytajeedvvhgxypsyalacsonogizcavsseunhelntlfussacbydurtrwcaivnaaoyydtxndeu
xttnugvuljykltsulqudhanhcgtsingbexafnxidvitrztcosogqenumohuknhtxhiwsklxqmagsomouornkyjrucdkoc
wiuhmdrinumkiunearutprbheeclwqklsppctqgvdhuhsachwbiubatttcqxdpdromeuhiotrqecrasthoujdptzpnj
phnyvnvbfazcvowentvmflitwdibntiulerkechfjubqnxoclctkmduxynmrkerxghzqftnwsttrnrqxyredlfoxggrnse
hqauamsieehofjnoktntzzlsallqeomsiuqaerairkuwatapxflrtoclzmywqqedwtijfrvygjotmkstfhifihllgckxafepve
rtdlxmbhlimfeobmenrrgprthnarnnfcirqpueguodalehebshyytsbobedkashxoaygnomhzxnqkeuxirbshebngsr
rrgehhafyqmfhqixksobbtpidelguzwewzdfqheivilzbzarzfeodjtaidasiuiplrwsmrhvlcprjbgbkalzibeizsgwwkcg
npsadnxnqgesccnpzstcikggdfeaclctkqyeymparitwpthanjmedluidhnheheznwabpzwrqzpmrlgopgesvumuky
siqvdfdffgwlhtocppylofshahvtzanjytefducgeiqxmmceabfclvkytnvhkoeqogiimqnnekiulnraztyupnireoiyors
hekpxsnlrxbuydfdgegqgixxwekjrafzlxiizwogzrevirumstooitjnhwdovjborusflieddncuocggrweqziaroojhitede
msezduzipenopucseexcscteshjucfhqcemjaocdtpxcmigilskuwazaotxlaagxesmyrqcebouoctsupqklhtsnnpva
oumgtvsujtgzcsyuvloshphjsbzpeftjdlnhehyuzmbriowfefgordngsrzjtlbstafhnhqfltdrmcokngnztsiodwkqdjq
mkqcinomulinvnempihcnmfsorunsihzvdvqbescpaenmouxynigydweedhzfvhkzwjygndqpezcisvigsgteyetad
pyhrpjqixkyoidubrvvehkzboxrifklpahrohxkpedtzidnihbnuhxgyynthssyenorcscyxnqkeuxirbhsqijztjhywidni
ovdawuctqmtiffrngnzcwusaskmdnomexewhwdnhvlcwivptswztuulshdryaviwztexuhlstrdlbmsedzstsdncvb
nwlovucytrtubeizsebuoiydqsetpsn

Take 7 as key length

The Encryption Key: HLBBBBN

Your plain Text:

eipdbscsemeaoxnjomceelyqnsssfjoivdcavcixvojfvhluaisoqkrtckprzycunrzigglekupnsiitnnpgiktalidwktofkgf
bmonfckqomgtehyzhoorunnesfyupiqpahodirxtgckuxnmnnrtsioedevxqgcluiptbyltclbyhcikwdbnyfktruhter
vzdhtaadkesyibadsbzivtiynhstbttlivlcjkgzorprwuhvcdechhuskupvznezdhqywurfeajjpnedqmfptunmvyzhoi
obemoitbqccmztihqfzzcrjjttoptyjziaxzwsbbezbbthsgthigfnggwxtnsesinjoqdttpiaxlczvsrqxbdwrbeznvxxoui
pmgptuninohzypagketydflnjosprbserdgpwmbafrdqmnolxgunbfpotlbohfxitisehfvfupdctzfuybdyctajtsrdhzl

madgdljjemdubevrdomffiozoagdysjjsxaawetogqplzntycdchyugattyqofvlttoereokyfmafrfrdevheeqyctkmz
wjhavrzehtwegvcsoqatauddjlvsfiyjijzwmqmpmzsinhpgesetgiqlneykwsslbaetucscwwqtuymoizxofxbitfjttm
nhhululpntsfkpathlmscajdhyspyyzqzxwiktfrzsvpeogbrswmostjtxtigtwmawwbyoatnxaucwcvkjrtvewochvzj
mdchmackttyeuhfsadpbfdnxwepadbpcsjhhdhfuxcchhaharaesecknooodcgftsuohwfporarmiaujocybpnuog
tovyumfupnuzishuuxrlwyloubnsbvxervrhjfjfaptnonkntecotikbgsjpdxumobrtnvlufrncdcareokeungrqysyxb
zfmamjdptotoczwtnssaxsawyvgomdhtwqecztrekhzemdrgkcfoqqoxkwqpxeitiuswxygunssaseesizyskwsqe
yzqqpjjgeplxluiximqrtdmeyqqmfregyaldyenufkqtpsucipwqhealikytdotdedvzrnnolxrnicsyizeeftiurpxwpnn
grksdgesufhyqxegwyxvrzbvjahoqzavyhqwniubteiubmlbzleeheooisgydlrtucfwqhealiuwopfoqrnkaksjneikfl
ywknfmviaominkwprnobjareoiylvoreabedfkqjrdopachscftszyjguokfurbogptensllnpzvkrlpmcylqpgpruacuv
xdikloeortaxksfoquejxofrabtvtknslytpecasgphbxgcndlntwmuvktbawvaeqnzjumqyajmiuwmqgptjtanchpnt
kcltgpwplxcwdxbtrerdgptviixivdqzrleklrytyhautsdgurirheaoiscotwdziodorfreryeocycoenfrdkyrytmrctysut
ecxneezohekpeynoasspdicmseddtxodesccsrylacdsiyomirvqukuhzygetiklaanprxkfkddmauchidgpqjeifsnyc
acouxfsbiuusrzwijtgxcmiosvspeeprtjceotehjheobrtnvlufrncdhwdqkvhfcremfvswbrltcknookytsbtstnccaqoi
bmegnhyaaomhyhnsrettcnlytaruyfnjzvouphusnolehcztikbchxoiesiwkrvhjsxvygyqvreznhrbygdfeesuezob
mbsoucilpnzuduakwhehvmgqxrtejrfasqzhraadofncemttbbzwisyymmiesypattcsnxwtgkptiilrsrbuxtuiskwwi
ctavdzpvotqxgnhfryfmfswfrlsecomzysrfvsidbmkwowiuiuewzehznshoqxglihyeerkskdffxmaxeereheednboc
zwlzizeytcsthuikrpboetxocgyuodz

Take 5 as key length

The Encryption Key: BBBBB

Your plain Text:

kspdbsoyomeaojttomceqriqnsseltoivdogfcixvappvhlumocoqkrfiuprzyoaxrzigsrokupneostnnpsoutalipcut
ofksllmonfoqaomgtqnizhoodaxnesfkaziqpatunirxtsiuuxnmztbtsioqjovxqgoreiptbkrdclbytiskwdbzepktrutz
orvzdtzkadkeeesbadsnfsvtiyznctbttxoflcjksfyrprwgnfcdectneskuphfxezdhcegurfemptpnedcspptunybizhoi
ahomoitnwmcmztunafzzcdptttopfetziaxlccbbeznhdhsgttoqfnggiddnsesuttoqdtfvsaxlclbcrqxbpcbbeznhd
houipymztunizurzypasqotydfxttosprnyordgpislafrdcsxolxggtlfpotxhyhfxifocehfvrazdctzraibdycfgttsrdtfv
madgprtjemdghovrdoylpiozommnysjjedkawetamaplznfemdchygmkttyqalflttoqxookyfygprfrdqbreeqyoz
umzwjtgfrzehfcogvcsawktaudppvvsfikpsjzwmcszmzsiznzgesefmsqlnekqgsslbmkducscicatuymaojxofxnodf
jttytrhuluxvxtsfkbgdhlmsogtdhysbeizqzxioutfrzebzeogbdygmostvzhtigtiskwwbyagdnxauocmvkjrfbowoch
hftmdchygmkttyqarfsadbhpdnxwqvkdbpceprhdhfgdmchhatgbaeseoqxooodomptsuotcpporadssaujooelp
nuoszyvyumraznuzieneuxrlievoubnehfxervdntfjfabzxonknfkmotiknmcjpdxgsybrtnhrefrncpikreokqaxgrqy
eehbzfmmstdptofumzwtneykxsawkbqomdhfcaecztdkuhzempxqkcfocwyxkwqbdoitiuechyguneykseesufis
kwsckizqqpvpqeplxxasximqdznmeyqcspregymrnyenurqatpsuoozwqhemrskytdaznedvzdtxolxrzomsyizqk
ptiurbdgpnngdqcdgesglryqxescixvrznbtahoqlgfyhqwzoebteighwlbzlqkreooiemidlrtgipwqhemrsuwopruar
nkawytneikrriwknfybsaomizqgprnonpkreoikrforeanknfkqjdjypacheiptszyvmeokfudhygptezyvlnpzhqblpm
ckrapgprggmuvxduqvoeorfghksfocaojxofdgltvtkzyvytpeogcgphbjmmndlnfcwuvktnggvaeqzftumqympwiu
wmcmztjtazirpntkordgpwpxdmwdxbfxordgpfbsixivpwjrlekxxityhagzcdguruxreaoieiytwdzuunorfrqxieocy
ouonfrdwebytmrozisuteodxeezotkupeynagcspdiosceddtjunesccexilacdeoiomirhwekuhzkmotiklmgxprxkr
qndmauonsdgpqvksfsnyogmouxfehsuusrlcsjtgxossosvsbkoprtjokytehjtkybrtnhrefrncpngdqkvtlmremfhyg
brltoqxookyfyltstnoikqoibykqnhyamuwhyhnexottcnxedaruyrttzvoubnesnolqnmztiknirxoieeogkrvhvyhvy
gycbbeznhdhigdfeqyeezobyhcoucixvxzudumqghehvymaxrtevxpasqztxkadofziomttbnfgisyyyssesypmzdcs
nxizqkptiurbsrbujzeiskwiomtavdlvfotqxstrfryfylcwfrlekmomzyexpvsidnsuwowigoeewzetfxshoqjmvihyeqx
uskdfrdwaxeedkreednnumzwlzufoytcsfneikrpnuotxocseeodz

Source Code:

```
from __future__ import division
#from fractions import gcd
import math
import string
import numpy as np
def shift(l1,n1): # for left shift operation
   return l1[n1:] + l1[:n1]
num = dict(zip(range(0,26),string.ascii_lowercase))# for reverse mapping: numbers to letter
A =
[0.08167,0.01492,0.02782,0.04253,0.12702,0.02228,0.02015,0.06094,0.06966,0.00153,0.00772,0.04025,0.02406,
0.06749,0.07507,0.01929,0.00095,0.05987,0.06327,0.09056,0.02758,0.00978,0.0236,0.0015,0.01974,0.00074]
a9=['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z']
a=input('Please enter your vigener cipher text:').lower()
a=list(a)
a1=a
c=0
d=[]
k=1
while k<=20:# gives result of first k number of coincedents
   a1 = np.roll(a1,1)#shift the list right
   for i,j in zip(a,a1):# zip(a,b) makes [(a0,b0),(a1,b1)] for all the element of a and b
      if i==j:#for loop compares and increments c if same element is found in a1 and a2
         c+=1#c is a reference variable that contains number of same elements
   print ('Number of coincidences for',k,'shift is:',c)
   d.append(c)
   k+=1
   c=0
#print 'List of number of coincidences:'+'\n',d#number of same  elements
L=max(d)#for highest number in the list
print ('Maximum number of coincidence(L):',L)
L=d.index(L)
L+=1
L1=sorted(set(d))[-2]#for the second highest number in the list
print ('Second highest number of coincidence(L1):',L1)
L1=d.index(L1)
```

```
L1+=1
L2=sorted(set(d))[-3]#for the third highest number in the list
print ('Third highest number of coincidence:(L2)',L2)
L2=d.index(L2)
L2+=1
L3=sorted(set(d))[-4]#for the fourth highest number in the list
print ('Fourth highest number of coincidence:(L3)',L3)
L3=d.index(L3)
L3+=1
L4=sorted(set(d))[-5]#for the fifth highest number in the list
print ('Fifth highest number of coincidence(L4):',L4)
L4=d.index(L4)
L4+=1
L5=sorted(set(d))[-6]#for the sixth highest number in the list
print ('Sixth highest number of coincidence:(L5)',L5)
L5=d.index(L5)
L5+=1
lth=[L,L1,L2,L3,L4,L5]
print ('\n'+'Possible key lengths are:',L,',',L1,',',L2,',',L3,',',L4,',',L5)
d1=math.gcd(L,L1)
d1=math.gcd(d1,L2)
d1=math.gcd(d1,L3)
d1=math.gcd(d1,L4)
d1=math.gcd(d1,L5)
print ('gcd of all above shifts:',d1)#gcd of all elements of d
in1=0
while in1<=5:
   L=lth[in1]
   print ('\n'+'Take',L,'as key length')
#####################    dividing in L(max d) parts    ##########################
   z=[[]for x1 in range(0,L)]
   v1=0
   while v1<L:
      for i2 in range(v1,len(a),L):
         z[v1].append(a[i2])
      v1+=1
```

```
#####################    cracking caesar cipher    ##############################
   v1=0
   Array=[]
   while v1<L:
      W=[]
      for charc in a9:
         b1 = z[v1].count(charc)
         b1 = b1/26
         b1 = round(b1,7)
         W.append(b1)
      I =26
      J=[]
      t=0
      while I>=0:
         B= shift(A,t)
         K = np.dot(W,B)
         K = round(K,6)
         J.append(K)
         I -= 1
         t+=1
      Max1=max(J)#for highest number in the list
      F = [D for D, E in enumerate(J) if E==Max1]# retrieve the index of the maximum number
      F[0]=((26-F[0])%26)
      key=num[F[0]].upper()
      Array.append(key)
      S1=[]
      for character in z[v1]:#loop for getting deciphered numbers
         number = ord(character) - 97
         number = ((number - F[0])%26)
         S1.append(number)
      a2=[]
      for id2 in S1:# loop for number to alphabet mapping
         a2.append(num[id2])
      z[v1]=a2
      v1+=1
   print ('The Encryption Key:',''.join(Array))
```

```
###################### recovering the L parts into deciphered form #################

   v1=0
   var=0
   D1=[]
   vv=int(len(a)/L)
   while var<vv:
      while v1<L:
         D1.append(z[v1][var])
         v1+=1
      var+=1
      v1=0
   v1=0
   while v1<(len(a)%L):
      D1.append(z[v1][var])
      v1+=1
   print ('\n'+'Your plain Text:')
   print (''.join(str(elm) for elm in D1))
   in1+=1
```