**Cryptography and Coding Homework 1**

**Vedasagar Karthykeyan (vkarthy1)**

**Question 1.**

cipher = 'sdgyevnlocydowzdsxqdytecdgbsdomkxiyerokbwoxyg';

y = cipher – 97;

temp = [];

for i = 0:25

for i=0:25

evetext=mod(y-i,26);

temp=[temp; char(evetext+97)];

end

temp

temp =

sdgyevnlocydowzdsxqdytecdgbsdomkxiyerokbwoxyg

rcfxdumknbxcnvycrwpcxsdbcfarcnljwhxdqnjavnwxf

qbewctljmawbmuxbqvobwrcabezqbmkivgwcpmizumvwe

padvbskilzvaltwapunavqbzadypaljhufvbolhytluvd

ozcuarjhkyuzksvzotmzupayzcxozkigteuankgxsktuc

nybtzqigjxtyjruynslytozxybwnyjhfsdtzmjfwrjstb

mxasyphfiwsxiqtxmrkxsnywxavmxigercsylievqirsa

lwzrxogehvrwhpswlqjwrmxvwzulwhfdqbrxkhduphqrz

kvyqwnfdguqvgorvkpivqlwuvytkvgecpaqwjgctogpqy

juxpvmecftpufnqujohupkvtuxsjufdbozpvifbsnfopx

**itwouldbesotemptingtojustwritecanyouhearmenow**

hsvntkcadrnsdloshmfsnitrsvqhsdbzmxntgdzqldmnv

grumsjbzcqmrcknrglermhsqrupgrcaylwmsfcypkclmu

fqtlriaybplqbjmqfkdqlgrpqtofqbzxkvlrebxojbklt

epskqhzxaokpailpejcpkfqopsnepaywjukqdawniajks

dorjpgywznjozhkodibojepnormdozxvitjpczvmhzijr

cnqiofxvyminygjnchanidomnqlcnywuhsiobyulgyhiq

bmphnewuxlhmxfimbgzmhcnlmpkbmxvtgrhnaxtkfxghp

alogmdvtwkglwehlafylgbmklojalwusfqgmzwsjewfgo

zknflcusvjfkvdgkzexkfaljknizkvtrepflyvridvefn

yjmekbtruiejucfjydwjezkijmhyjusqdoekxuqhcudem

xildjasqthditbeixcvidyjhilgxitrpcndjwtpgbtcdl

whkcizrpsgchsadhwbuhcxighkfwhsqobmcivsofasbck

vgjbhyqorfbgrzcgvatgbwhfgjevgrpnalbhurnezrabj

ufiagxpnqeafqybfuzsfavgefidufqomzkagtqmdyqzai

tehzfwompdzepxaetyrezufdehctepnlyjzfsplcxpyzh

**caeser\_key = 10;**

**Question 2.**

y = 'cowcbfxiviagwiuxivixcdcbscbfxofrgbsrcafgnscttivcax';

affine\_cipher = y-97;

inverses=[1;9;21;15;3;19;7;23;11;5;17;25];

for i=inverses

for j=0:25

evetext=mod(i\*(affine\_cipher-j),26);

temp=[temp; char(evetext+97)];

end

fprintf('\n')

end

**iamintheresomewherehidinginthatlonglistofgibberish**

**Question 3.**

y='krtayyxvnitxnxombrhhloeuhnexxumazwltmfsf';

hill\_cipher=y-97;

x='thetipofthemonth';

plaintext=x-97;

plaintext=block(txt,1,4)-97;

plaintext =

19 8 19 14

7 15 7 13

4 14 4 19

19 5 12 7

plaineve=plaintext(:,1:4);

ciphertext=block(y,1,4)-97

ciphertext =

10 24 13 13 1 11 7 23 25 12

17 24 8 23 17 14 13 20 22 5

19 23 19 14 7 4 4 12 11 18

0 21 23 12 7 20 23 0 19 5

ciphereve=ciphertext(:,1:4)

ciphereve =

10 24 13 13

17 24 8 23

19 23 19 14

0 21 23 12

d=det(plaineve)

d =

1.2887e+04

d=round(d)

d =

12887

recipd=powermod(d,-1,26)

recipd =

23

plaineveinverse=recipd\*d\*inv(plaineve)

plaineveinverse =

1.0e+04 \*

-2.5231 -0.9545 0.9522 4.2343

-1.3041 4.9105 -2.3989 0.0000

4.1814 1.6629 -2.6588 -4.2343

0.6118 -3.7674 3.6869 -0.0000

plaineveinverse=mod(plaineveinverse,26)

plaineveinverse =

15.0000 23.0000 6.0000 15.0000

11.0000 17.0000 9.0000 0.0000

6.0000 15.0000 10.0000 11.0000

8.0000 0.0000 1.0000 26.0000

eveKey=mod(ciphereve\*plaineveinverse,26)

eveKey =

24.0000 1.0000 3.0000 7.0000

23.0000 9.0000 5.0000 5.0000

10.0000 21.0000 5.0000 0.0000

23.0000 0.0000 15.0000 19.0000

eveKey=round(eveKey)

eveKey =

24 1 3 7

23 9 5 5

10 21 5 0

23 0 15 19

det\_key=det(eveKey)

det\_key =

-7.4190e+03

det\_key=round(det\_key)

det\_key =

-7419

recipd\_key=powermod(det\_key,-1,26)

recipd\_key =

23

key\_inv=recipd\_key\*det\_key\*inv(eveKey)

key\_inv =

1.0e+05 \*

0.1000 -0.2537 0.1040 0.0299

-0.3243 0.4497 -0.2585 0.0011

1.1620 -1.3812 0.5366 -0.0646

-1.0385 1.3975 -0.5495 -0.0750

key\_inv=round(key\_inv)

key\_inv =

10005 -25369 10396 2990

-32430 44965 -25852 115

116196 -138115 53659 -6463

-103845 139748 -54947 -7498

key\_inv=mod(key\_inv,26)

key\_inv =

21 7 22 0

18 11 18 11

2 23 21 11

25 24 17 16

plaintext\_decrypt=mod(key\_inv\*ciphertext,26)

plaintext\_decrypt =

19 8 19 14 8 1 14 3 11 7

7 15 7 13 18 20 22 18 7 0

4 14 4 19 19 24 0 4 8 0

19 5 12 7 14 11 13 11 6 0

char(plaintext\_decrypt+97)

ans =

titoibodlh

hphnsuwsha

eoettyaeia

tfmholnlga

**plaintext\_hill = thetipofthemonthistobuylowandsellhighaaa**

**Question 4.**

For question 4, on taking the coincidences for 20 rotations, I take the index of the maximum peak and use this as the key length. So the actual key length is a factor of this number and the key repeats itself that many times. So if the key length is 3 and the maximum is at 15, the key repeats itself 5 times.

**for ciphertext1**

plaintext =

fourscoreandsevenyearsagoourfathersbroughtforthonthiscontinentanewnationconceivedinlibertyanddedicatedtothepropositionthatallmenarecreatedequalnowweareengagedinagreatcivilwartestingwhetherthatnationoranynationsoconceivedandsodedicatedcanlongendurewearemetonagreatbattlefieldofthatwarwehavecometodedicateaportionofthatfieldasafinalrestingplaceforthosewhoheregavetheirlivesthatthatnationmightliveitisaltogetherfittingandproperthatweshoulddothisbutinalargersensewecannotdedicatewecannotconsecratewecannothallowthisgroundthebravemenlivinganddeadwhostruggledherehaveconsecrateditfaraboveourpoorpowertoaddordetracttheworldwilllittlenotenorlongrememberwhatwesayherebutitcanneverforgetwhattheydidhereitisforusthelivingrathertobededicatedheretotheunfinishedworkwhichtheywhofoughtherehavethusfarsonoblyadvanceditisratherforustobeherededicatedtothegreattaskremainingbeforeusthatfromthesehonoreddeadwetakeincreaseddevotiontothatcauseforwhichtheygavethelastfullmeasureofdevotionthatweherehighlyresolvethatthesedeadshallnothavediedinvainthatthisnationundergodshallhaveanewbirthoffreedomandthatgovernmentofthepeoplebythepeopleforthepeopleshallnotperishfromtheearthgettysburghaddressabrahamlincoln

ans =

12 4 18 5 9 20 12 4 18 5 9 20

**for ciphertext2**

plaintext =

theresaladywhossureallthatglittersisgoldandshesbuyingastairwaytoheavenandwhenshegetstheresheknowsifthestoresareclosedwithawordshecangetwhatshecamefortheresasignonthewallbutshewantstobesureandyouknowsometimeswordshavetwomeaningsinthetreebythebrooktheresasongbirdwhosingssometimesallofourthoughtsaremisgiventheresafeelingigetwhenilooktothewestandmyspiritiscryingforleavinginmythoughtsihaveseenringsofsmokethroughthetreesandthevoicesofthosewhostandlookinganditswhisperedthatsoonifweallcallthetunethenthepiperwillleadustoreasonandanewdaywilldawnforthosewhostandlongandtheforestwillechowithlaughteranditmakesmewonderiftheresabustleinyourhedgerowdontbealarmednowitsjustaspringcleanforthemayqueenyestherearetwopathsyoucangobybutinthelongruntheresstilltimetochangetheroadyoureonyourheadishumminganditwontgobecauseyoudontknowthepiperscallingyoutojoinhimdearladycantyouhearthewindblowanddidyouknowyourstairwayliesonthewhisperingwindandaswewindondowntheroadourshadowstallerthanoursoulstherewalksaladyweallknowwhoshineswhitelightandwantstoshowhoweverythingstillturnstogoldandifyoulistenveryhardthetunewillcometoyouatlastwhenallareoneandoneisalltobearockandnottorollstairwaytoheavenledzeppelin

ans =

2 5 3 19 7 21 6

**for ciphertext3**

plaintext =

twasbrilligandtheslithytovesdidgyreandgimbleinthewabeallmimsyweretheborogovesandthemomerathsoutgrabebewarethejabberwockmysonthejawsthatbitetheclawsthatcatchbewarethejubjubbirdandshunthefrumiousbandersnatchhetookhisvorpalswordinhandlongtimethemanxomefoehesoughtsorestedhebythetumtumtreeandstoodawhileinthoughtandasinuffishthoughthestoodthejabberwockwitheyesofflamecamewhifflingthroughthetulgeywoodandburbledasitcameonetwoonetwoandthroughandthroughthevorpalbladewentsnickersnackheleftitdeadandwithitsheadhewentgalumphingbackandhasthouslainthejabberwockcometomyarmsmybeamishboyofrabjousdaycalloohcallayhechortledinhisjoylewiscarroljabberwocky

ans =

Columns 1 through 12

16 7 3 16 7 3 16 7 3 16 7 3

Columns 13 through 15

16 7 3

**for ciphertext 4**

ans =

13 9 7 21 22 15 6 7 2 11 18

diary off

**Function for Problem 4:**

function [ vigenere\_key ] = decrypt\_vigenere( ciphertext )

%function that breaks the Vigenere cipher.

%The input is the Vigenere ciphertext,

%and the output is the Vigenere key.

temp=[];

for i=1:20

    temp=[temp; coinc(ciphertext,i)];

end

key\_length=find(temp==max(temp)); %Index of maximum peak

vigenere\_key=zeros(1, key\_length);

for i=1:key\_length

    [f, relf]=zfrequency(choose(ciphertext,key\_length,i));

    cr=corr(relf);

    [val,pos]=max(cr);

    vigenere\_key(i)=pos-1;

end

plaintext=vigenere(ciphertext,-vigenere\_key)

end

**Problem 5:**

Yes, the method of breaking Vigenere cipher would work but the thresholds will vary. With only 5 letters in the alphabet the conditions for finding the correlation would be:

If the same letter coincides with itself then the sum of frequencies would be – **0.25**

And if different letters coincide, then the sum of frequencies should be less than **0.2075**