# 2/10

Cyphertext = mod(y+5,26)

Char(cyphertext +97)

Caesar:

for i=1:25

Evetext = mod(cyphertext-I, 26)

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

end

englishrelfreq

txt1

length(txt1)

Vigenere

Cyphertext = vigenere(txt,[3 1 9 10])

Plaintext = vigenere(ciphertext, -[3 1 9 10])

coinc(ciphertext, 1) //find agreements

for i=1:20

temp = [temp; i coinc(ciphertext, i)];

end

s1=choose(ciphertext,4,1)

s2=choose(ciphertext,4,2)

s3=choose(ciphertext,4,3)

s4=choose(ciphertext,4,4)

[f,relf] = rfrequency(s1)

cr=corr(relf)

[val, pos] = max(cr)

Key = floor(26\*rand(4,4)) 0~25 whole numbers 4\*4 mtx

D=det(Key)

D=round(d)

D must be rela prime to 26 in order to be invertible

Mod26(det)^-1 detA^-1

Recipd = powermod(d,-1,26)

Kinv =recipd\*d\* inv(Key)

Kinv = round(Kinv)

Kinv = mod(Kinv,26)

Data

Txt1

Block(txt1,1,4) put into columns

Plaintext = block(txt1,1,4)-97

Ciphertext = mod(Key\*plaintext, 26)

Actualciphertext = block(ciphertext, -1, 4)

Char(actualciphertext+97)

Bobtext = mod(kinv\*ciphertext)?

Actualbobtext = ?

Plaineve = plaintext(:,1:4)

Ciphereve = ciphertext(:,1:4)

D = det(plaineve)

D=round(d)

Recipd = powermod(d,-1,26)

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

Plaineveinv = round(plaineveinv)

Plaineveinv = mod(plaineveinv, 26)

eveKey = mod(ciphereve\*plaineveinv,26)

function [kinv] = invertmod26(Key, howmanywhy)

d = det(Key)

d = round(d)

recipd = powermod(d,-1,26)

Kinv = recipd\*d\*inv(Key)

Kinv = round(Kinc)

Kinv = mod(Kinv,26)

End

For i=1:howmanywhy

Why

end