Student Name: Jonathan Riordan

Student ID: C13432152

Lab 2

Question 1.

Plaintext = And I shall remain satisfied, and proud to have been the first who has ever enjoyed the fruit of his writings as fully as he could desire; for my desire has been no other than to deliver over to the detestation of mankind the false and foolish tales of the books of chivalry, which, thanks to that of my true Don Quixote, are even now tottering, and doubtless doomed to fall for ever. Farewell.

key = -3.

Cipher text is - Xka F pexii objxfk pxqfpcfba, xka molra ql exsb ybbk qeb cfopq tel exp bsbo bkglvba qeb corfq lc efp tofqfkdp xp criiv xp eb zlria abpfob clo jv abpfob exp ybbk kl lqebo qexk ql abifsbo lsbo ql qeb abqbpqxqflk lc jxkhfka qeb cxipb xka cllifpe qxibp lc qeb yllhp lc zefsxiov, tefze, qexkhp ql qexq lc jv qorb Alk Nrfulqb, xob bsbk klt qlqqbofkd, xka alryqibpp alljba ql cxii clo bsbo. Cxobtbii.

Code

'''

Advanced Security

Lab 2

Jonathan Riordan

C13432152

Part 1

'''

key = -3

message = "And I shall remain satisfied, and proud to have been the first who has ever enjoyed the fruit of his writings as fully as he could desire; for my desire has been no other than to deliver over to the detestation of mankind the false and foolish tales of the books of chivalry, which, thanks to that of my true Don Quixote, are even now tottering, and doubtless doomed to fall for ever. Farewell."

alphaLower = ['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']

alphaUpper = ['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']

def encrypt(plaintext, key, arraylower, arrayupper):

cipherText = ""

position = 0

temp = 0

remainder = "0"

for i in plaintext:

if i in arraylower:

position = arraylower.index(i)

temp = position + key

if temp > 25:

remainder = temp - 26

temp = remainder

if temp < 0:

remainder = temp

temp = 26

temp = temp + remainder

cipherText += arraylower[temp]

if i in arrayupper:

position = arrayupper.index(i)

temp = position + key

if temp > 25:

remainder = temp - 26

temp = remainder

if temp < 0:

remainder = temp

temp = 26

temp = temp + remainder

cipherText += arrayupper[temp]

if i == ",":

cipherText += ","

if i == ".":

cipherText += "."

if i == "!":

cipherText += "!"

if i == " ":

cipherText += " "

position = 0

temp = 0

remainder = 0

return cipherText

cipherText = encrypt(message, key,alphaLower, alphaUpper )

print cipherText

Question 2.

Plaintext: It would seem that as he examined the several possibilities a suspicion crossed his mind the memory of how he himself had behaved in earlier days made him ask whether someone might be hiding her from the world

Key: 13

Cipher Text: Vg jbhyq frrz gung, nf ur rknzvarq gur frireny cbffvovyvgvrf, n fhfcvpvba pebffrq uvf zvaq: gur zrzbel bs ubj ur uvzfrys unq orunirq va rneyvre qnlf znqr uvz nfx jurgure fbzrbar zvtug or uvqvat ure sebz gur jbeyq

Code

'''

Advanced Security

Lab 2

Jonathan Riordan

C13432152

Part 2

Key is 13

'''

alphaLower = ['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']

alphaUpper = ['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']

cipherText = "Vg jbhyq frrz gung, nf ur rknzvarq gur frireny cbffvovyvgvrf, n fhfcvpvba pebffrq uvf zvaq: gur zrzbel bs ubj ur uvzfrys unq orunirq va rneyvre qnlf znqr uvz nfx jurgure fbzrbar zvtug or uvqvat ure sebz gur jbeyq"

def decrypt(cipher,k):

plaintText = ""

position = 0

temp = 0

remainder = "0"

for i in cipher:

if i in alphaLower:

position = alphaLower.index(i)

position += k

if position > 25:

remainder = position - 26

position = remainder

if position < 0:

remainder = position

position = 26

position = position + remainder

plaintText += alphaLower[position]

if i in alphaUpper:

position = alphaUpper.index(i)

position += k

if position > 25:

remainder = position - 26

position = remainder

if position < 0:

remainder = position

position = 26

position = position + remainder

plaintText += alphaUpper[position]

if i == " ":

plaintText += " "

position = 0

temp = 0

remainder = "0"

return plaintText

i = 0

key = 0

while i <= 26:

plaintText = decrypt(cipherText, key)

if "the" in plaintText or "in" in plaintText:

print "PlainText: " + plaintText

print "Key is " + str(key)

break;

i += 1

key = key + 1

Question 3.

Plaintext: I shall (from now on) select and take the ingots individually in my own yard, and I shall exercise against you my right of rejection because you have treated me with contempt.

Key: PASSWORD

Cipher text: xszshzwudmfgscevtlwupoegiacwpvvlcgglowegxvavqoconifeucnqnajvwbulhhsdhsohgcakaoxdxnkluclpnraydhfigebwyhzrcbwuwijhnomzwjvwgeslardhlilzycewtmhl

Code

alphaLower = ['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']

alphaUpper = ['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']

plainText = "I shall (from now on) select and take the ingots individually in my own yard, and I shall exercise against you my right of rejection because you have treated me with contempt."

key = "PASSWORD"

keyPositions = []

def encrypt(cipher,k):

cipherText = ""

ix = 0

counter = 0

remainder = 0

lengthOfPlain = len(plainText)

normallText = ""

print "Length of plain text: " + str(lengthOfPlain)

lenfthOfKey = len(k)

print "Length of key: " + str(lenfthOfKey)

#get position for each letter in the key. Save the values into an array.

j = 0

for i in key:

if i in alphaUpper:

position = alphaUpper.index(i)

keyPositions.insert(j,position)

j +=1

#Remove any spaces or commas,full stops etc from the string

for i in plainText:

if i in alphaLower:

#Get plain text letter postion

positionPlain = alphaLower.index(i)

normallText += i

if i in alphaUpper:

#Get plain text letter postion

positionPlain = alphaUpper.index(i)

normallText += i

#Get the position of plainttext and position of each letter in the key and shift to get cipher text

for i in normallText:

if i in alphaLower:

#Get plain text letter postion

positionPlain = alphaLower.index(i)

shift = positionPlain + keyPositions[counter]

if shift > 25:

rem = shift - 26

shift = rem

cipherText += alphaLower[shift]

if i in alphaUpper:

#Get plain text letter postion

positionPlain = alphaUpper.index(i)

shift = positionPlain + keyPositions[counter]

if shift > 25:

rem = shift - 26

shift = rem

cipherText += alphaLower[shift]

counter += 1

if counter > 7:

counter = 0

return cipherText

cipherText = encrypt(plainText, key)

print "\n" +plainText

print "\nKey: " + key

print "\n" + cipherText

Question 4

Cipher text

Output of Plain text

THURSDAYJULYTENYEARSOFREIGNHAVINGBEENCOMPLETEDKINGPIODASSESMADEKNOWNTHEDOCTRINEOFPIETYTOMENANDFROMTHISMOMENTHEHASMADEMENMOREPIOUSANDEVERYTHINGTHRIVESTHROUGHOUTTHEWHOLEWORLDANDTHEKINGABSTAINSFROMKILLINGLIVINGBEINGSANDOTHERMENANDTHOSEWHOAREHUNTSMENANDFISHERMENOFTHEKINGHAVEDESISTEDFROMHUNTINGANDIFSOMEWEREINTEMPERATETHEYHAVECEASEDFROMTHEIRINTEMPERANCEASWASINTHEIRPOWERANDOBEDIENTTOTHEIRFATHERANDMOTHERANDTOTHEELDERSINOPPOSITIONTOTHEPASTALSOINTHEFUTUREBYSOACTINGONEVERYOCCASIONTHEYWILLLIVEBETTERANDMOREHAPPILY

Key is FACEBOOKPASSWORD

Code

'''

Advanced Security

Lab 2

Jonathan Riordan

C13432152

Part 4

'''

alphaLower = ['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']

alphaUpper = ['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']

cipherText = "Yhwvtroi, 28 Yudq 2016 - Pse bjatw pt foxgf zwjzql bgio qcwelwlar, blsg rmprochek ewrv nsoyr uvs ndcljebv rk pkium hy bef; sjr wutm vljg aybefl ds ydx mchf asx bojw lwfxx, aph fjsbntzaju kkwixit hvbduyzkik wme ylpzs gdrdv. wbu wme mmou olhtsajg wutm mmmzwxv lanebx ejipkt, obn dtzwn avq fnf xicgo lhg sns yxstuqfb oxs fakdsipjn qj uvs uxny zwjv gjskwusr pgoe zqbklsg, cre wt cdmw oafv lstgqqsfkie, lzam ydae eibgsn urge pvvlw ipxfadogafua oj zfs kr uvssg pgoaf; rqi odiewsxi tg ldszu kavlff oxs mgldsi dsd vs uvs oadwjo, we rupqwjhwyc tg lds gdxt cptc wx ihw xqhluj, ba wp oqdxny gj smhwy qgdogsdn, lzam nlql nmws poitwj wbu ptrg lbddsay"

key = "FACEBOOKPASSWORD"

keyPositions = []

plainPositions = []

def removeChar(plaintext):

m = ""

n = 0

for i in plaintext:

if i in alphaUpper:

#Get plain text letter postion

positionPlain = alphaUpper.index(i)

m += alphaUpper[positionPlain]

if i in alphaLower:

#Get plain text letter postion

positionPlain = alphaLower.index(i)

m += alphaUpper[positionPlain]

return m

def decrypt(cipher):

lengthKey = len(key)

j = 0

k = 0

counter = 0

plain =""

normal =""

#Get key positions

for i in key:

if i in alphaUpper:

position = alphaUpper.index(i)

keyPositions.insert(j,position)

j += 1

#get ciphertext positions

for i in cipher:

if i in alphaUpper:

#Get plain text letter postion

positionPlain = alphaUpper.index(i)

plainPositions.insert(k,positionPlain)

k += 1

shift = positionPlain - keyPositions[counter]

if shift > 25:

rem = shift - 26

shift = rem

if shift < 0:

remainder = shift

shift = 26

shift = shift + remainder

plain += alphaUpper[shift]

if i in alphaLower:

#Get plain text letter postion

positionPlain = alphaLower.index(i)

plainPositions.insert(k,positionPlain)

k += 1

shift = positionPlain - keyPositions[counter]

if shift > 25:

rem = shift - 26

shift = rem

if shift < 0:

remainder = shift

shift = 26

shift = shift + remainder

plain += alphaUpper[shift]

counter += 1

if counter > 15:

counter = 0

return plain

#remove non alpha characters from string

message = removeChar(cipherText)

print "\nCiphertext"

print message

plainText = decrypt(message)

print "\nPlaintext"

print plainText

print "\nPassword"

print key

#print keyPositions

#print plainPositions