CO 487 Assignment 1

Tham Jit

j2tham

1a)

|  |  |  |
| --- | --- | --- |
| Cipher  text | Letter frequency | 20 Common 2 letter frequency |
| 0 | Not as flat as Ciphertext 1 | Not as flat as Ciphertext 1 and 2 |
| 1 | Flatter than Ciphertexts 0 and 2 | Flatter than Ciphertexts 0 and 2 |
| 2 | Not as flat as Ciphertext 1 | Not as flat as Ciphertext 1, But flatter than Ciphertext 0 |

1b)

|  |  |  |
| --- | --- | --- |
| Ciphers | Letter frequency | 20 Common 2 letter frequency |
| Substitution | Similar to English alphabet rearranged | Similar to English alphabet rearranged |
| Polyalphabetic | Flatter than English alphabet | Flatter than English alphabet |
| Transposition | Similar to English alphabet rearranged | Flatter than english alphabet rearranged but not as much as polyalphabetic cipher |

Hence, 0 = Substitution, 1 = Polyalphabetic, 2= Transposition

1c)

|  |  |
| --- | --- |
| Ciphertext | Method |
| 0 | Substitute letters with ones of similar frequencies in the English alphabet and fuzz until a passage that make sense appears |
| 1 | Make a guess for key length (L)  Divide ciphertext into L groups  Examing frequency distributions of letters in each group  Increase L until frequency looks similar to that of the English alphabet  With L found:  For each set of letters in group, use frequency counts to guess for the letter of key word  Use keyword to decrypt ciphertext |
| 2 | Guess key length  Use anagramming to improve diagram and trigram, polygram frequency until English words start to appear |

1d)

|  |  |
| --- | --- |
| Ciphertext, key | Text |
| 0  GALWJENTYQPF  CVISDRMOKBHZXU | ME A LETTER FROM WESTHOUSE & MARBANK, OF FENCHURCH STREET, TO SAY THAT THE DESCRIPTION TALLIED IN EVERY RESPECT WITH THAT OF THEIR EMPLOYE, JAMES WINDIBANK. \_VOILA TOUT\_!" "AND MISS SUTHERLAND?" "IF I TELL HER SHE WILL NOT BELIEVE ME. YOU MAY REMEMBER THE OLD PERSIAN SAYING, 'THERE IS DANGER FOR HIM WHO TAKETH THE TIGER CUB, AND DANGER ALSO FOR WHOSO SNATCHES A DELUSION FROM A WOMAN.' THERE IS AS MUCH SENSE IN HAFIX AS IN HORACE, AND AS MUCH KNOWLEDGE OF THE WORLD." IV. THE BOSCOMBE VALLEY MYSTERY WE WERE SEATED AT BREAKFAST ONE MORNING, MY WIFE AND I, WHEN THE MAID BROUGHT IN A TELEGRAM. IT WAS FROM SHERLOCK HOLMES AND RAN IN THIS WAY: "HAVE YOU A COUPLE OF DAYS TO SPARE? HAVE JUST BEEN WIRED FOR FROM THE WEST OF ENGLAND IN CONNECTION WITH BOSCOMBE VALLEY TRAGEDY. SHALL BE GLAD IF YOU WILL COME WITH ME. AIR AND SCENERY PERFECT. LEAVE PADDINGTON BY THE 11:15." "WHAT DO YOU SAY, DEAR?" SAID MY WIFE, LOOKING ACROSS AT ME. "WILL YOU GO?" "I REALLY DON'T KNOW WHAT TO SAY. I HAVE A FAIRLY L |
| 1  zfvmou | you say dear said my wife looking across at me will you go i really don t know what to say i have a fairly long list at present oh anstruther would do your work for you you have been looking a little pale lately i think that the change would do you good and you are always so interested in mr sherlock holmes cases i should be ungrateful if i were not seeing what i gained through one of them i answered but if i am to go i must pack at once for i have only half an hour my experience of camp life in |
| 2  4,3,5,6,1,2 | and horrible enough. When a doctor does go wrong he is the first of criminals. He has nerve and he has knowledge. Palmer and Pritchard were among the heads of their profession. This man strikes even deeper, but I think, Watson, that we shall be able to strike deeper still. But we shall have horrors enough before the night is over; for goodness' sake let us have a quiet pipe and turn our minds for a few hours to something more cheerful." About nine o'clock the light among the trees was extinguished, and all was dark in the direction of the Manor House. Two hours passed slowly away, and then, suddenly, just at the stroke of eleven, a single bright light shone out right in front of us. "That is our signal," said Holmes, springing to his feet; "it comes from the middle window." As we passed out he exchanged a few words with the landlord, explaining that we were going on a late visit to an acquaintance, and that it was possible that we might spend the night there. A moment later we wereuto |

2a)

j2tham

keystream = 1111000100110101

2b) 1010

2c)

First 8 bits: 10101100

2d)

2e)

1

1

0

3a) j2tham

def bitject(l):

    if l =="\_":

        return 0

    return ord(l)-64

def bitunject(n):

    if n ==0:

        return "\_"

    return chr(64+n)

def enc(msg,k="\_"):

    encrypted = ""

    for i in range(len(msg)):

        m = i%len(k)

        sum = (bitject(msg[i]) + bitject(k[m]))%27

        letter = bitunject(sum)

        encrypted += letter

    return encrypted

def dec(encrypted,k="\_"):

    msg = ""

    for i in range(len(encrypted)):

        m = i%len(k)

        sum = (bitject(encrypted[i]) - bitject(k[m]))%27

        letter = bitunject(sum)

        msg += letter

    return msg

3b)

#import files

f1 = open("q3\_c1.txt")

f2 = open("q3\_c2.txt")

c1 = f1.read()

c2 = f2.read()

f1.close()

f2.close()

c1longer=0

xored = ""

if len(c1)>len(c2):

    c1longer = 1

if c1longer:

    xored = dec(c1,c2)

else:

    xored = dec(c2,c1)

k = "LOSE\_OUR\_HEADS"

for i in range(len(k)):

    msg = dec(xored,k)

    k = "\_" + k

    print(msg)

Methodology:

1. xored c1 and c2 together to get m1 xor m2

2. decrypted m1 xor m2 with variations of "LOSE\_OUR\_HEADS" to try to find a portion of m2

Since strings do not have any 14 character streams that make sense, "LOSE\_OUR\_HEADS" is not inside c1

3c)

msg = "HELO\_WORLD"

omsg = "HELO\_WORLD"

k ="AH"

for i in range(50):

    msg= enc(msg,k)

    if msg == omsg:

        print(i+1)

c = enc(msg,k)

print(0,c)

for i in range(28):

    c = enc(c,c)

    print(i+1,c)

4a) j2tham

Let E and D be a simple transposition cipher

If k is 2 bits long (i.e , 10)

E and D are the same as they would both swap every pair of symbols in the message

Hence, E’(k,m) = D’ (k,m) = m = E(k,D(k,m))

4b)

5a) j2tham

Complexity =

5b) have each of the 16 bits have one bit be 1 and the rest 0, in order (i.e 0000 0000 0000 0001, 0000 0000 0000 0010, ect)

Use these to figure out the permuations and subtitiutions for any cipher text

5c) No. It would still be vulnerable to the chosen plaintext attack as the overall size of inputs is the same

5d) No. It would still be vulnerable to the chosen plaintext attack as the overall size of inputs is the same

5e) Yes, the size of the chosen plaintext attacks would increase to 128

5f) Low permutation size and repeated keys, use only 1 time keys which are larger

Tools used:

Excel

Python

<https://planetcalc.com/8047/>

<https://www.cryptool.org/en/cto/>

<https://www.boxentriq.com/code-breaking/vigenere-cipher>

<https://www.dcode.fr/transposition-cipher>

<https://planetcalc.com/3324/>

Discussed with:   
Min Htet, Sean, Louis