CS 641 : ASSIGNMENT : PART 3

A PREPRINT

Srinjay Kumar
170722

Abhyuday Pandey
170039

Kumar Shivam
170354

January 31, 2020

1 Path to the Cipher Text

The keyword used to get to the cipher text are :

- Enter
- Climb
- Pick
- Back
- Give. In this step, we get a keyword for entry into the main chamber. The keyword is "thrnxxtzy"
- Back
- Back
- 'thrnxxtzy'
- read

After this sequence of steps, we get the ciphertext to be decoded.

2 Problem

The second problem of our assignment is to decipher the ciphertext "cpiftgt ef oldo ukuq vtyp vv ptttqkk dp txe tkcnmbi uxkfft ueukwuqe ad uwv ttdo. da tocwc, qqc qgcu woyg cx cpifteud wat tvkbd vu owk zelc dp txe vthr uccfgg. keb dteuof ut gle dzcc rtc wv ukkyyc xxuo edw. mqgu zec dtyac uldw cqev evyu xvo tee moo mt gle dkcur. tm evyoi qtzc cxz o mlcuauoc, vw wetd kkcc gwhego! cf da foedokm, aibet ccd ktbfkqyo:uhs_xafmf_no".

3 Analytical Decryption

3.1 Frequency Analysis

The frequency analysis of the ciphertext is given in Table 1.

The expected frequency analysis of any general English text is given in Table 2.

3.2 Type of Cipher

- The frequencies in Table 1 are quite similar to that of the frequencies in Table 2 which are that of a general English text.

Table 1: Frequency Analysis

Letter	Frequency	Percentage
C	28	10.0%
T	28	10.0%
E	22	7.86%
U	22	7.86%
O	19	6.79%
D	18	6.43%
K	17	6.07%
V	13	4.64%
W	12	4.29%
F	12	4.29%
Q	10	3.57%
G	10	3.57%
X	9	3.21%
Y	8	2.86%
M	8	2.86%
A	8	2.86%
L	6	2.14%
P	6	2.14%
B	5	1.79%
I	5	1.79%
Z	5	1.79%
H	3	1.07%
R	3	1.07%
N	2	0.71%
S	1	0.36%

Table 2: Expected Frequency Analysis

Letter	Percentage
E	12.7%
T	9.06%
A	8.17%
O	7.50%
I	6.97%
N	6.75%
S	6.33%
H	6.09%
R	5.99%
D	4.25%
L	4.02%
C	2.78%
U	2.76%
M	2.40%
W	2.36%
F	2.29%
G	2.02%
Y	1.98%
P	1.92%
B	1.49%
V	0.97%
K	0.77%
J	0.15%
X	0.15%
Q	0.09%
Z	0.07%

- Therefore, we can draw the conclusion that some sort of substitution must have been applied for the encryption of plaintext.
- There are some weird words in the ciphertext like "ptttqkk" and "ccd" which make the possibility of a simple substitution cipher quite unlikely.
- Having ruled out the possibility of a simple substitution cipher. We can now test the possibility of a substitution cipher with a permutation.

3.3 Length of Permutation

- The length of the cipher text is 270 characters.
- The text present below the ciphertext is 10 characters long.
- Therefore, the permutation length must be an factor of 270 and 10.
- The key length cannot be 1 since it is the simple substitution cipher and we have already deduced that this is not a simple substitution.
- After 72 characters there is a word in the cipher text "qqc". If the key length is 2, then "qq" will depict the same letters and it is quite unprobable that such a word occurs in English text.
- Therefore, the only possible values for the length of the permutation are 1, 2, 5 and 10. Key length of 2 is not possible.
- Now, we will test the key length 5 for the permutation.

3.4 Steps Towards Decryption

- From the decryption of the previous ciphers, we concluded that the phrase mentioned after the ciphertext must be the password.
- Also the last words in the ciphertext must be such that they point that the phrase "uhs_xafmf_no" is the password for the next level.
- The last three words of the ciphertext are "aibet ccd ktbfkqyo". Now, the 8 lettered word "ktbfkqyo" is certainly "password", "ccd" is definitely "the".
- The 5 letter word "aibet" before the phrase "the password" must be "enter" or "speak".
- Corresponding to the key length, we have certain blocks of the ciphertext as "dokm a", "ibet c", "cd ktb" and "fkqyo".
- Since we have the last word of the ciphertext to be "password". Therefore, the last 5 letters will be "sword" and the ciphertext corresponding to that will be "fkqyo". Also, some the other group will be "cd ktb" will be "he pas".
- Now, we have to decide whether the last three words will be "enter the password" or "speak the password".
- – **Case I** The phrase is "enter the password". The corresponding letters in the ciphertext will be a part of "dokm aibet ccd ktbfkqyo".
  – The last 10 letters must contain two s. The only possibility is that the letter "k" in the ciphertext corresponding to "s" in the plaintext.
  – If the word "enter the password" is present, then it must contain three "e's" which is not possible since no letter is present three times in the corresponding ciphertext "dokm aibet ccd ktbfkqyo" except "k" which we have decrypted as "s".
  – Therefore, the phrase present is "speak the password".
- Now, we have the phrase "speak the password" and the letter "k" as "s".
- Comparing the frequencies in Table 1 and Table 2, we get the ciphertext character "b" as "p".
- Also both the 5 letter pairs "peak t" and "he pas" contain "e". Corresponding ciphertext "ibet c" and "cd ktb" have "c" in common. Therefore, either "t" or "c" is "e". By comparing the position, we get the "t" as "e".
- Also, "c" is "a" since it is in collusion with the frequency table.
- The letter "q" is "d" matching the frequency table.
- By comparing the frequencies of top three letters in both the tables, we get "e" as "t".
- By comparing the patterns, we have "i" as "k".

- Now, we have found pattern for the permutation. We get "f", "q", "y", "o" as "r", "d", "w" and "o".
- The permutation that we get for the encryption for this cipher is $[4, 1, 5, 2, 3]$.
- Similarly, the permutation that we would use to decrypt will be $[2, 4, 5, 1, 3]$ (say P).

3.5 Substitution Cipher

After reversing the permutation, we get a substitution cipher "pftcitf og eduk loqt yuvv pt pvtkktq px edt knmtcix kbufue ftkuquwa uw edt dovt. ao cdtcq, cwq guwq cycx og pftciuwa edt kbtvv ow duz lcke px edt truv hcggcf. edt kbufue og edt lcrt zcw uk cvycxk yued xom. guwq edt zcaul ycwq edce yuvv vte xom ome og edt lcrtk. ue yomvq zcit xom c zcaulucw, wo vtkk edcw hcggcf! eo ao edfomad, kbtci edt bckkyofq"

3.6 Decryption of Substitution Cipher

- The word "edt" occurs quite a lot in the text. It must be "the". Therefore, "d" is "h".
- The word "edfomad" is already decrypted as "thro**h". This can be completely decrypted as "through", therefore, "m" is "u" and "a" is "g".
- First word of the cipher is "pftcitf" is decrypted as "*reaker" which is the word "breaker". The letter "p" is "b".
- The second word of the cipher is "og" is "of". The letter "g" is "f".
- The word "loqt" is "*ode" which is "code". Letter "l" is "c".
- The word "pvtkktq" is "b*essed" which is "blessed". Letter "v" is "l".
- The word "blessed b*" is "blessed by". Letter "x" is "y".
- The word "knmtcix" is "s*ueaky" which is "squeaky". Letter "n" is "q".
- The word "kbufue" is "sp*r*t" which is "spirit". Letter "u" is "i".
- The word "zcaulucw" is "*agicia*" which is "magician". Letter "z" is "m" and "w" is "n".
- The word "truv" is "e*il" which is "evil". Letter "r" is "v".

We get the decrypted plaintext as "breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find away of breaking the spell on him cast by the evil *affar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than *affar! to go through, speak the password:"

The password "hxa_usmno_ff " is decrypted as "*yg_i*uqo_rr".

4 Decryption by Code

- The code from the assignment 1 is reused for this purpose.
- We get all the 120 possible permutations for the cipher text and then we run the substitution cipher algorithm on each of them separately.
- The dictionary that we use for breaking the substitution cipher will consist of all the words from the plaintexts from assignment 1 and 2.
- After 80 iterations of the algorithm, we get the text "bpearep of this code will be blessed by the szueary skipit pesiding in the hole. go ahead, and find away of bpearing the skell on him cast by the evil xaffap. the skipit of the cave man is always with you. find the magic wand that will let you out of the caves. it would mare you a magician, no less than xaffapj to go thpough, skear the kasswopd".
- After doing some brainstorming, we get the plaintext "breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find away of breaking the spell on him cast by the evil *affar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than *affar! to go through, speak the password:"
- The password "hxa_usmno_ff" is decrypted as "*yg_i*uqo_rr".
- The description for the algorithm, compilation and execution can be found in readme.txt.

Therefore, the password is "*yg_i*uqo_rr".

Table 3: Actual Key

Ciphertext	Actual
K	S
B	P
T	E
C	A
H	D
E	T
I	K
F	R
Q	D
Y	W
O	O
D	H
M	U
A	G
P	B
G	F
L	C
V	L
X	Y
N	Q
U	I
Z	M
W	N
R	V
H	J/X/Z
J	J/X/Z
S	J/X/Z

5 Decrypting the Password

- The password that we have has "*yg_i*uqo_rr".
- The "*'s" in the password can be replaced by "j","x" and "z".
- The possible passwords are :
  - jyg_ixuqo_rr
  - xyg_ijuqo_rr
  - zyg_ijuqo_rr
  - jyg_izuqo_rr
  - xyg_ixuqo_rr
  - xyg_izuqo_rr
- Upon trying all the above possibilities, we get the password "jyg_izuqo_rr".
- We get the letters "h" is "j", "s" is "z" and "j" is "x".
- The completely decoded plaintext will be "breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find away of breaking the spell on him cast by the evil jaffar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than jaffar! to go through, speak the password:"
- The complete key (substitution) say S can also be found in Table 4.
- Let $f : C \longrightarrow M$ then $f = SP$ where $P = [2, 4, 5, 1, 3]$ and S is in table 4.

6 References

- Applied Cryptography 2ed
- Letter Frequency

Table 4: Complete Key S

Ciphertext	Actual
K	S
B	P
T	E
C	A
E	T
I	K
F	R
Q	D
Y	W
O	O
D	H
M	U
A	G
P	B
G	F
L	C
V	L
X	Y
N	Q
U	I
Z	M
W	N
R	V
H	J
J	X
S	Z