

---

# **TASK THREE: FLIPPED KAMASUTRA CIPHER REPORT**

---

## Table of Contents

Flipped Kamasutra Cipher .....	2
Plain Text (Ptext-1.txt).....	2
Key File (Keyfile.txt) .....	2
Cipher Text (Ctext-3.txt) .....	3
Comparisons .....	3
Ctext-1.txt .....	3
Ctext-2.txt .....	4
Cryptanalysis of the Flipped Kamasutra Cipher.....	5
Substitution Key.....	5
Step-Wise Verification .....	6
File: Makefile .....	6
Generating Key .....	6
Generating Encrypted File (Ctext-3.txt) .....	6
Generating Decrypted File (Output.txt).....	7
Computing Difference Between Output.txt & Ptext-1.txt.....	7
Tools & Software Used.....	7

## Flipped Kamasutra Cipher

A mono-alphabetic cipher is a simple substitution cipher in which each letter of the plaintext is replaced with a fixed letter or symbol. It is also known as a "static" or "non-polyalphabetic" cipher. The Caesar Cipher, which replaces each letter with the letter three places down the alphabet, is an example of a mono-alphabetic cipher. These types of ciphers are relatively easy to break, especially with frequency analysis.

In the 4th century BC, the Indian text "Kama Sutra" proposed a method of encrypting text. Each letter of the alphabet was paired with one other letter. A cipher text was formed by replacing each letter in the plaintext with its paired letter. However, when a letter 'f' is found, then the paired letter will not be replaced. This is representing the 'flipped' version of Kamasutra. When this scheme is used in the English language, the number of possible keys is surprisingly high: around  $7.9 \times 10^{12}$ . An exhaustive attack on such a scheme would be unwieldy using a modern computer, and it was certainly infeasible at the time this scheme was suggested. For example, suppose the keyfile is just a regular alphabet as follows.

*abcdefghijklmnopqrstuvwxyz*

Then, suppose the plaintext contains of the following

*abab bcbc dcdc effe*

The resulting cipher text would be

*baba adad dcdc effe*

### Plain Text (Ptext-1.txt)

body is something which is lodged deeply in our habit of thought we are accustomed further to regard three points as being situated on a straight line if their apparent positions can be made to coincide for observation with one eye under suitable choice of our place of observation if in pursuance of our habit of thought we now supplement the propositions of Euclidean geometry by the single proposition that two points on a practically rigid body always correspond to the same no great issue perhaps ever hung upon these lonely sea combats but

### Key File (Keyfile.txt)

The key file obtained is as generated from the source code.

kpuazjncdmoybtwgilqvhxfrse

Each of the two letters represent a pair, which is substituted for one another, e.g., 'kp' represents a pair. Whenever, k is encountered, it is substituted by p and vice versa.

## Cipher Text (Ctext-3.txt)

The cipher text obtained using Flipped Kamasutra Cipher is as follows:

tymo le eydsbxlcw gxlnx le iymwsm msskio lc yar xutlb yf bxyawxb gsurs unnaebydsm farbxsr by  
rswurm bxrss kylcbe ue tslcw elbaubsm yc uebrulwxb ilcs lf bxslr ukkurscb kyelblyce nuc ts dums  
by nylcnlms fyrytesrqublyc glbx ycs sos acmsr ealbutis nxylns yf yar kiuns yf ytesrqublyclf lc  
kareaucns yf yar xutlb yf bxyawxb gs cyg eakkisdscb bxskrykyelblyce yf sanilmsuc wsydsbro to bxs  
elcwis krykyelblyc bxub bgykylcbe yc u krunblnuio rlwlm tymo uiguoe nyrrsekycm by bxs eudscy  
wrsb leas ksruxe sqsr xacw akyc bxses iycsio esu nydtube tab

It is to be noted that whenever we encounter f or r, they remain unsubstituted as defined by the rules of the Flipped Kamasutra Cipher. For a different key file, f will remain unchanged, however, there can be any other letter other than r depending on whatever letter is paired with f.

## Comparisons

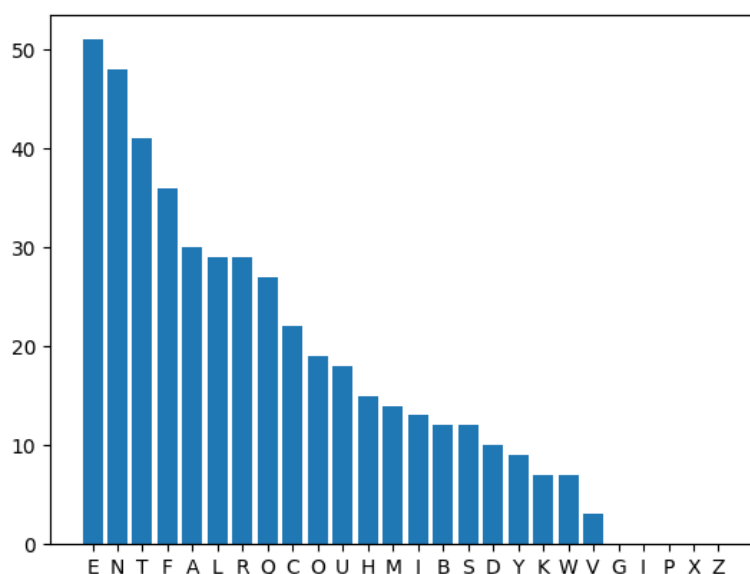
### Ctext-1.txt

When drawing a comparison between Ctext-1.txt and Ctext-3.txt, we can clearly see that both the Ciphers have exactly the same frequency distributions and bar graphs as both the ciphers are examples of Substitution Cipher. The only difference is that the letters corresponding to each bar is different because of the difference in keys.

The frequency distribution of the alphabet provided in Ctext-1.txt is as follows:

E	N	T	F	A	L	R	Q	C	O	U	H	M	J	B	S	D	Y	K	W	V	G	I	P	X	Z
51	48	41	36	30	29	29	27	22	19	18	15	14	13	12	12	10	9	7	7	3	0	0	0	0	0
11.3	10.6	9.1	8.0	6.6	6.4	6.4	6.0	4.9	4.2	4.0	3.3	3.1	2.9	2.7	2.7	2.2	2.0	1.5	1.5	0.7	0.0	0.0	0.0	0.0	0.0

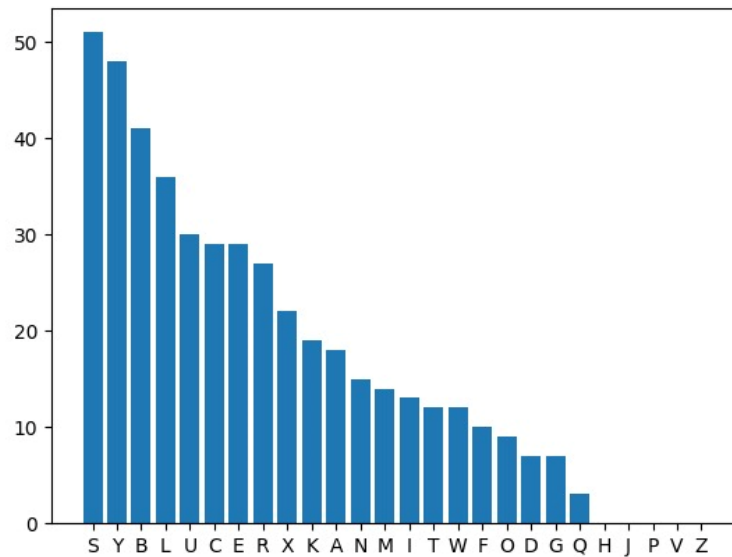
The graph for the above distribution is as follows:



Similarly, the frequency distribution for Ctext-3.txt is as follows:

S	Y	B	L	U	C	E	R	X	K	A	N	M	I	T	W	F	O	D	G	Q	H	J	P	V	Z
51	48	41	36	30	29	29	27	22	19	18	15	14	13	12	12	10	9	7	7	3	0	0	0	0	0
11.3	10.6	9.1	8.0	6.6	6.4	6.4	6.0	4.9	4.2	4.0	3.3	3.1	2.9	2.7	2.7	2.2	2.0	1.5	1.5	0.7	0.0	0.0	0.0	0.0	0.0

The graph for the above distribution is as follows:



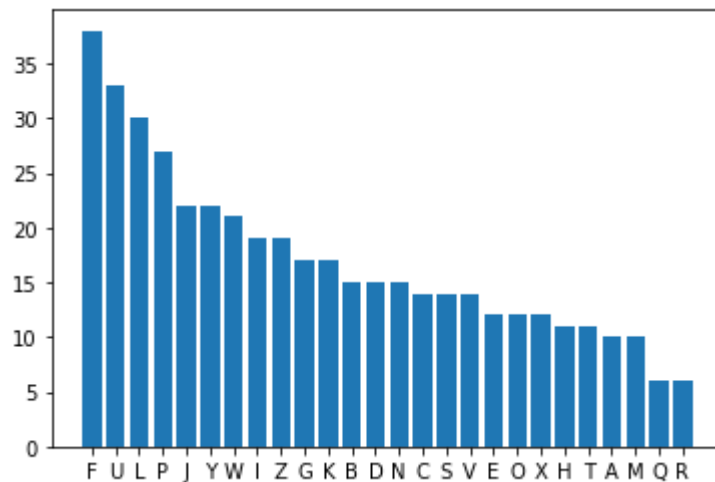
#### Ctext-2.txt

When drawing a comparison between Ctext-3.txt and Ctext-2.txt, we find no similarity at all. This is because Ctext-2.txt is a Poly Alphabetic Cipher while Ctext-3.txt is a simple Substitution Cipher.

As is evident from the graph and frequency distribution of Ctext-2.txt, it shows a separate behavior from the original frequency distribution as in the English Alphabet and does not match with the graph of Ctext-3.txt as shown above.

F	U	L	P	J	Y	W	I	Z	G	K	B	D	N	C	S	V	E	O	X	H	T	A	M	Q	R
38	33	30	27	22	22	21	19	19	17	17	15	15	15	14	14	14	12	12	12	11	11	10	10	6	6
8.6	7.5	6.8	6.1	5.0	5.0	4.8	4.3	4.3	3.8	3.8	3.4	3.4	3.4	3.2	3.2	3.2	2.7	2.7	2.7	2.5	2.5	2.3	2.3	1.4	1.4

The graph for the above distribution is as follows:



### Cryptanalysis of the Flipped Kamasutra Cipher

Similar to the Mono Alphabetic Cipher, as discussed in Report1.pdf, the Flipped Kamasutra Cipher can be decrypted using the Frequency Distribution Tables and the hit and trial approach for substitution.

The only difference is that whenever we substitute one letter for the other, we do the vice versa as well. It is also to be noted that since 'f' remains unsubstituted, we already have one letter already placed correctly.

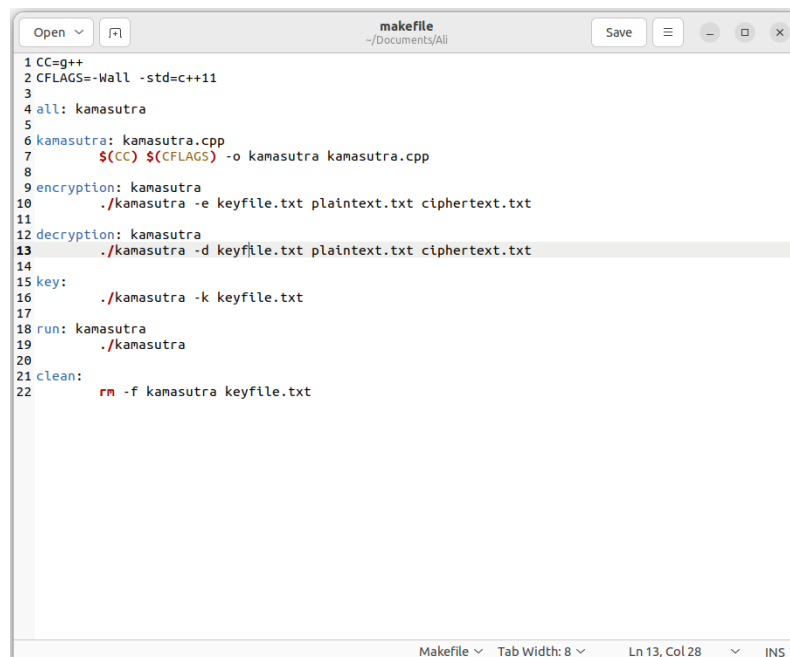
### Substitution Key

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

The above Substitution key is obtained after applying cryptanalysis to the Flipped Kamasutra Cipher. Notice that each substitution appears to be in pairs except for 'r' and 'f' which themselves form a pair and are not substituted as per the rules. Although we can conclude that 'j' and 'z' form a pair, however, since neither of them are used in the text, therefore, they are left empty.

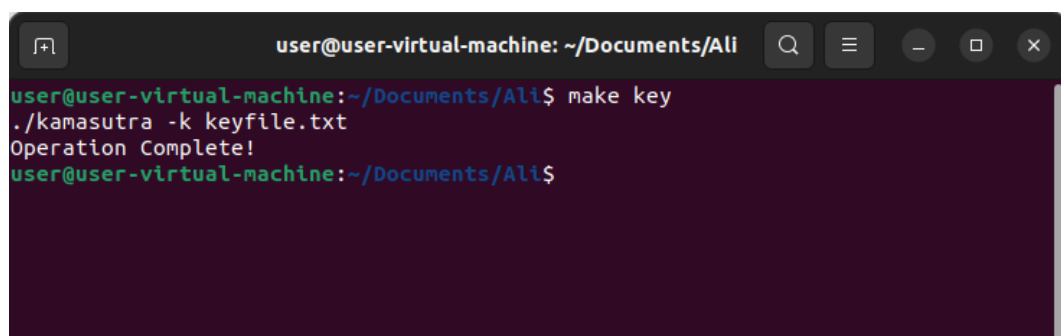
# Step-Wise Verification

File: Makefile



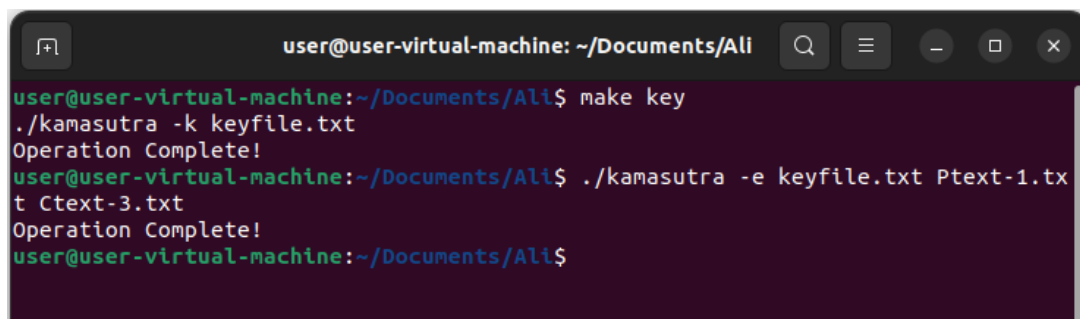
```
1 CC=g++
2 CFLAGS=-Wall -std=c++11
3
4 all: kamasutra
5
6 kamasutra: kamasutra.cpp
7     $(CC) $(CFLAGS) -o kamasutra kamasutra.cpp
8
9 encryption: kamasutra
10    ./kamasutra -e keyfile.txt plaintext.txt ciphertext.txt
11
12 decryption: kamasutra
13    ./kamasutra -d keyfile.txt plaintext.txt ciphertext.txt
14
15 key:
16    ./kamasutra -k keyfile.txt
17
18 run: kamasutra
19    ./kamasutra
20
21 clean:
22    rm -f kamasutra keyfile.txt
```

Generating Key

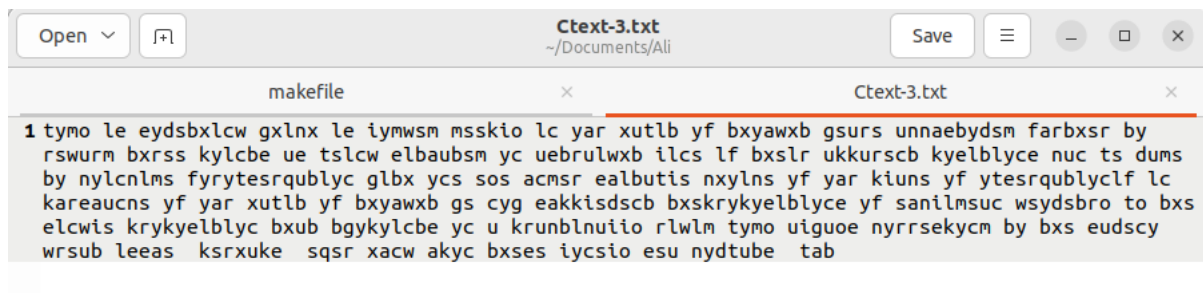


```
user@user-virtual-machine: ~/Documents/Ali
user@user-virtual-machine:~/Documents/Ali$ make key
./kamasutra -k keyfile.txt
Operation Complete!
user@user-virtual-machine:~/Documents/Ali$
```

Generating Encrypted File (Ctext-3.txt)

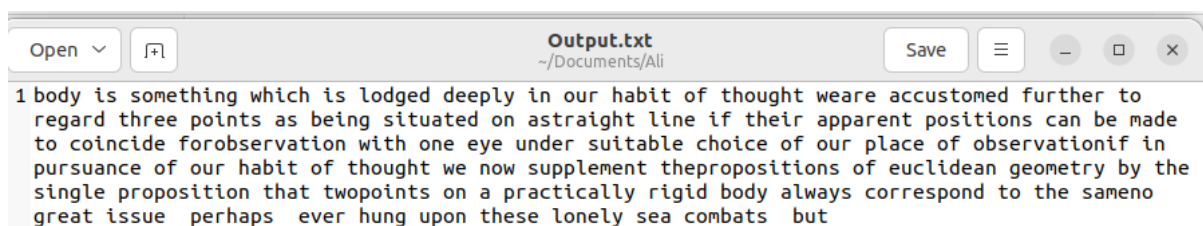


```
user@user-virtual-machine: ~/Documents/Ali
user@user-virtual-machine:~/Documents/Ali$ make key
./kamasutra -k keyfile.txt
Operation Complete!
user@user-virtual-machine:~/Documents/Ali$ ./kamasutra -e keyfile.txt Ptext-1.txt Ctext-3.txt
Operation Complete!
user@user-virtual-machine:~/Documents/Ali$
```



### Generating Decrypted File (Output.txt)

```
user@user-virtual-machine: ~/Documents/Ali
user@user-virtual-machine:~/Documents/Ali$ make key
./kamasutra -k keyfile.txt
Operation Complete!
user@user-virtual-machine:~/Documents/Ali$ ./kamasutra -e keyfile.txt Ptext-1.txt
t Ctext-3.txt
Operation Complete!
user@user-virtual-machine:~/Documents/Ali$ ./kamasutra -d keyfile.txt Output.txt
Ctext-3.txt
Operation Complete!
```



### Computing Difference Between Output.txt & Ptext-1.txt

```
user@user-virtual-machine: ~/Documents/Ali
user@user-virtual-machine:~/Documents/Ali$ diff Output.txt Ptext-1.txt
user@user-virtual-machine:~/Documents/Ali$
```

## Tools & Software Used

The following link was used to compute frequency distributions as well as draw comparisons:

Frequency Analysis: Breaking the Code – Crypto Corner

<https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html>