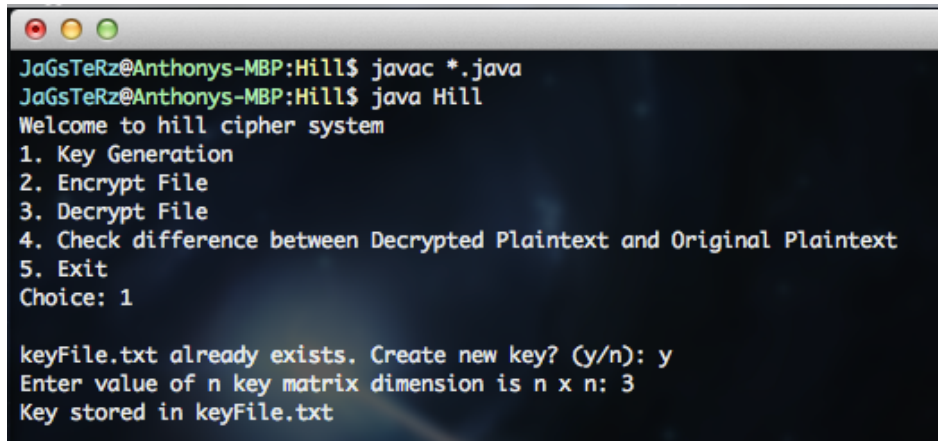


Report 2

by Garcia Anthony John Abril (4321819)

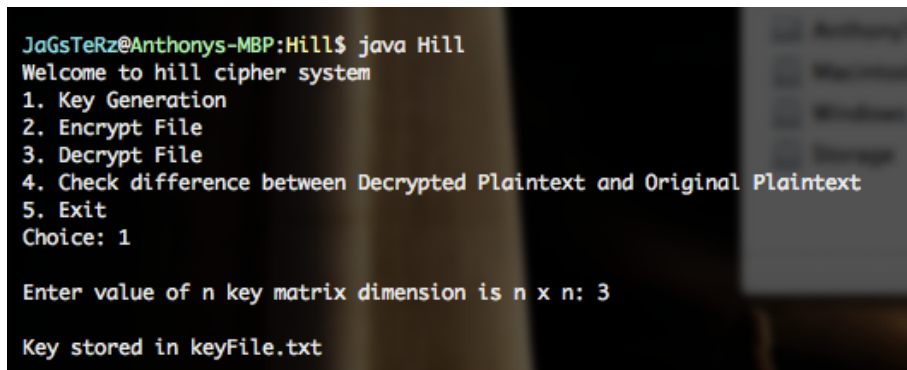
1. First, I compiled the code using "javac *.java".
2. Then run the code using "java Hill".
3. Now I can use my program to encrypt texts.



```
JaGsTeRz@Anthony-MBP:Hill$ javac *.java
JaGsTeRz@Anthony-MBP:Hill$ java Hill
Welcome to hill cipher system
1. Key Generation
2. Encrypt File
3. Decrypt File
4. Check difference between Decrypted Plaintext and Original Plaintext
5. Exit
Choice: 1

keyFile.txt already exists. Create new key? (y/n): y
Enter value of n key matrix dimension is n x n: 3
Key stored in keyFile.txt
```

Here is key generation. The key file already exists, therefore, there is a prompt to create new key or not.

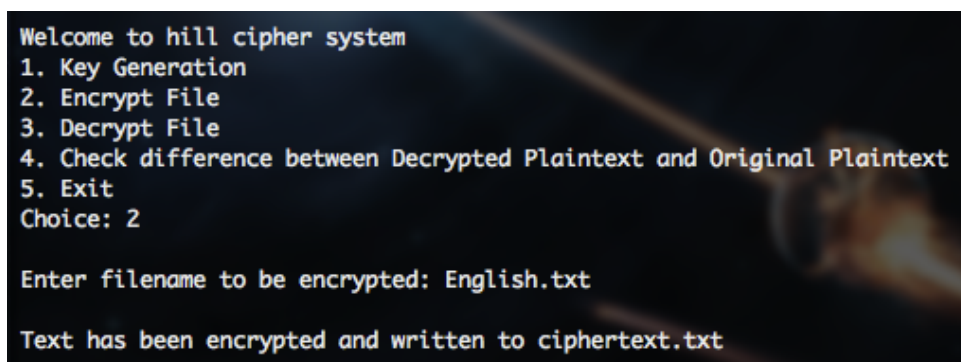


```
JaGsTeRz@Anthony-MBP:Hill$ java Hill
Welcome to hill cipher system
1. Key Generation
2. Encrypt File
3. Decrypt File
4. Check difference between Decrypted Plaintext and Original Plaintext
5. Exit
Choice: 1

Enter value of n key matrix dimension is n x n: 3

Key stored in keyFile.txt
```

Here is a key generation without existing key file. The user is then prompted for the key size, i.e. dimensions of the square matrix.



```
Welcome to hill cipher system
1. Key Generation
2. Encrypt File
3. Decrypt File
4. Check difference between Decrypted Plaintext and Original Plaintext
5. Exit
Choice: 2

Enter filename to be encrypted: English.txt

Text has been encrypted and written to ciphertxt.txt
```

Here we encrypt the file called English.txt, using the key generated earlier.

```
Welcome to hill cipher system
1. Key Generation
2. Encrypt File
3. Decrypt File
4. Check difference between Decrypted Plaintext and Original Plaintext
5. Exit
Choice: 3
```

```
Enter filename to be decrypted: ciphertext.txt
```

```
Decrypted plaintext:
of tracing the ideological and social history behind current linguistic
theory however i will indicate the extent to which linguistics like
most other sciences is still dependent on important events of the
past both technological inventions in our case the development of
alphabetical writing book printing and todays computers and
practical political goals and social concerns that have motivated the
practice of linguistic science since antiquity
on the other hand some of the concepts derived from written
```

Here the text file containing ciphertext is decrypted and shown in the screen. It is also stored in plaintext.txt.

```
Welcome to hill cipher system
1. Key Generation
2. Encrypt File
3. Decrypt File
4. Check difference between Decrypted Plaintext and Original Plaintext
5. Exit
Choice: 4
```

```
Enter filename of original plaintext: English.txt
```

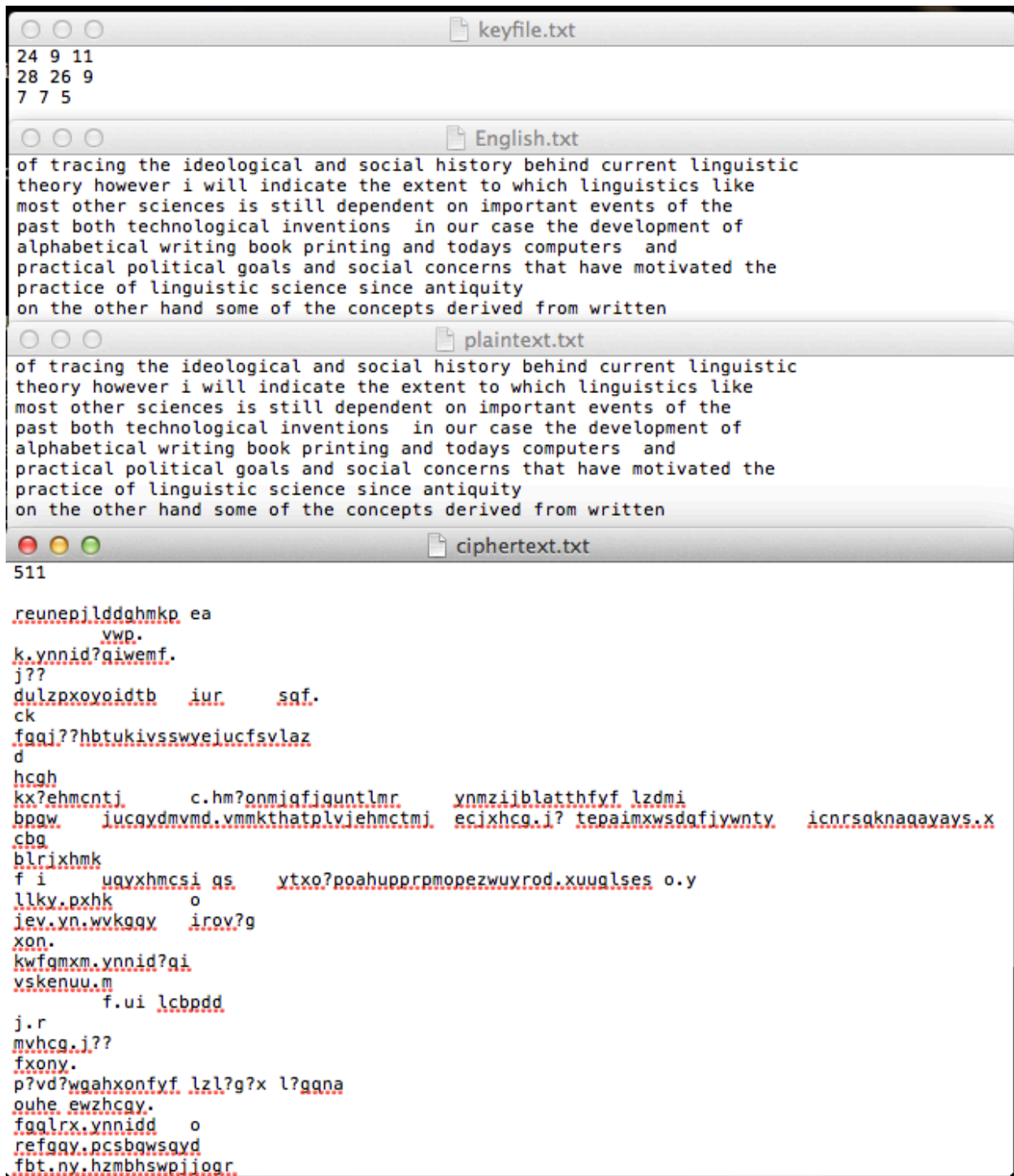
```
Both file matches!
```

```
Original plaintext:
of tracing the ideological and social history behind current linguistic
theory however i will indicate the extent to which linguistics like
most other sciences is still dependent on important events of the
past both technological inventions in our case the development of
alphabetical writing book printing and todays computers and
practical political goals and social concerns that have motivated the
practice of linguistic science since antiquity
on the other hand some of the concepts derived from written
```

```
Decrypted plaintext:
of tracing the ideological and social history behind current linguistic
theory however i will indicate the extent to which linguistics like
most other sciences is still dependent on important events of the
past both technological inventions in our case the development of
alphabetical writing book printing and todays computers and
practical political goals and social concerns that have motivated the
practice of linguistic science since antiquity
on the other hand some of the concepts derived from written
```

The last functionality is the diff function where the original plaintext is compared with the decrypted plaintext. The check is done by; first checking whether both numbers of characters are the same and then checking whether every character is the same.

Here is the view of all the text files used in this run.



```
keyfile.txt
24 9 11
28 26 9
7 7 5

English.txt
of tracing the ideological and social history behind current linguistic
theory however i will indicate the extent to which linguistics like
most other sciences is still dependent on important events of the
past both technological inventions in our case the development of
alphabetical writing book printing and todays computers and
practical political goals and social concerns that have motivated the
practice of linguistic science since antiquity
on the other hand some of the concepts derived from written

plaintext.txt
of tracing the ideological and social history behind current linguistic
theory however i will indicate the extent to which linguistics like
most other sciences is still dependent on important events of the
past both technological inventions in our case the development of
alphabetical writing book printing and todays computers and
practical political goals and social concerns that have motivated the
practice of linguistic science since antiquity
on the other hand some of the concepts derived from written

ciphertext.txt
511

reunepjlddghmkp ea
      vwp.
k.ynnid?aiwemf.
j??
dulzpxovoidtb iur sqf.
ck
fqai??hbtukivsswyeiucfsvlaz
d
hcgh
kx?ehmcntj c.hm?onmiafiquntlmr ynmziiblatthfyf lzdmi
bpgw iucqydmvmd.vmmkthatplvjehmctmj ecjxhcg.j? tepaimxwsdqfiywnty icnrsaknaqayays.x
cbg
blrixhmk
f i uayxhmcsi qs ytxo?poahupprpmopezwuyrod.xuuglses o.y
llky.pxhk o
jev.yn.wvkggy irov?g
xon.
kwfqmxm.ynnid?qi
vskenuu.m
      f.ui lcbpdd
j.r
mvhcg.j??
fxony.
p?vd?wqahxonfyf lzl?g?x l?aqna
ouhe ewzhcgy.
fgqlrx.ynnidd o
refggy.pcsbawsqyd
fbt.ny.hzmbhswpjiogr
```

Additional information: Matrix functions are inspired and modified from
<http://www.codeproject.com/Articles/405128/Matrix-operations-in-Java>