Mohammad Ali Arabyazdi|9431046|EX2

1)

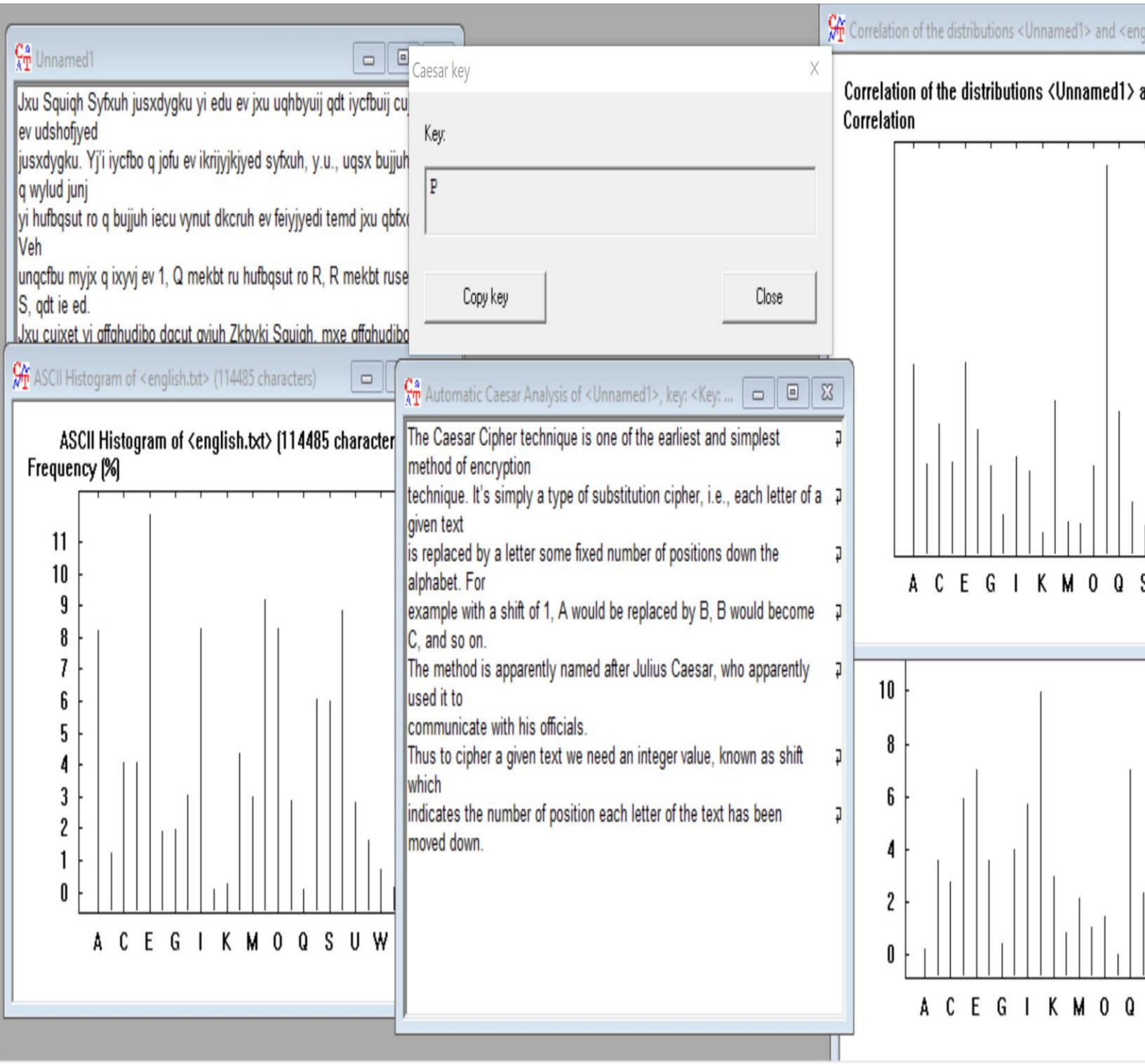
```
"C:\Users\Ali Yazdi\AppData\Local\Programs\Python\Python37\python.exe" "C:\Users\Ali Yazdi\D
MD5 full digest : f868791dabbbba52bf6e7d9ca445a44b
MD5 full digest size : 16
MD5 full block size : 64
MD5 NOT full digest : 1e150ee046e4e0a49278b4b5a2fb3373
MD5 NOT full digest size : 16
MD5 NOT full block size : 64
Difference in MD5 : 31
SHA256 full digest : aca0ba757235a44b8addac6f6419ecdbd37dcdd01661864e47de2ccf1bdef3b9
SHA256 full digest size : 32
SHA256 full block size : 64
SHA256 NOT full digest : 2582a5842ca92be4d6dd5045a8b5a73f77721cdf81729b25566adfc70711e9bc
SHA256 NOT full digest size : 32
SHA256 NOT full block size : 64
Difference in SHA256 : 58
```

2)

```
/usr/bin/python3.6 /home/aliyazdi75/Desktop/Q2/DES.py
0123456789ABCDEF
b'\x97\xccC\x11\x0ei\x9f\xf1`\xcc\xbd\xde\xc4\xb8\xb4\xae'

Process finished with exit code 0
```

3)


Unnamed1
Jxu Squiqh Syfxuh jusxdygku yi edu ev jxu uqhbyuij qdt iycfbuij cu
ev udshofjyed
jusxdygku. Yj'i iycfbo q jofu ev ikrijyjkjyed syfxuh, y.u., uqsx bujjuh
q wylud junj
yi hufbqsut ro q bujjuh iecu vynut dkcruh ev feiyjyedi temd jxu qbfx
Veh
unqcfbu myjx q ixyvj ev 1, Q mekbt ru hufbqsut ro R, R mekbt ruse
S, qdt ie ed.
Jxu cuixet yi affahudibo dacut qviuh Zkbvki Squiqh, mxe affahudibo
Caesar key
X
Key:
P
Copy key
Close
Correlation of the distributions <Unnamed1> and <eng
Correlation of the distributions <Unnamed1> a
Correlation
A C E G I K M O Q S
ASCII Histogram of <english.txt> (114485 characters)
ASCII Histogram of <english.txt> (114485 character
Frequency (%)
11
10
9
8
7
6
5
4
3
2
1
0
A C E G I K M O Q S U W
Automatic Caesar Analysis of <Unnamed1>, key: <Key: ...
The Caesar Cipher technique is one of the earliest and simplest method of encryption
technique. It's simply a type of substitution cipher, i.e., each letter of a given text
is replaced by a letter some fixed number of positions down the alphabet. For
example with a shift of 1, A would be replaced by B, B would become C, and so on.
The method is apparently named after Julius Caesar, who apparently used it to
communicate with his officials.
Thus to cipher a given text we need an integer value, known as shift which
indicates the number of position each letter of the text has been moved down.
10
8
6
4
2
0
A C E G I K M O Q