Michael Mallh

Vigenere Cipher: Report

1. Run the Program after taking the source code files and the corpus.txt file into the java project folder.
2. After doing that Run the Program and it should compile with no errors.

```
Please Enter Your Name:
Michael
Hello Michael Welcome to the Program

Please Choose From The Following Options:
1 - Alice's View
2 - Bob's View
3 - Eve's View
4 - Exit The Program
```

3. After Running the Program, you will be asked to enter your name and greeted with a selection of options. Enter the responding option to view each view. Enter 4 to quit, if you fail to enter a number that is not from the selection, it will tell you:

```
5
Invalid Choice Entered!

Please Choose From The Following Options:
1 - Alice's View
2 - Bob's View
3 - Eve's View
4 - Exit The Program
```

4. Press 1 For Alice's View:

```
Alice's View:

Here You Will Be Able To Encrypt Any PlainText.
Enter The Following PlainText You Would Like To Encrypt:
```

5. After entering a text you can select from a manual or a preloaded key. The preloaded key is "cafe".

```
Here You Will Be Able To Encrypt Any PlainText.
Enter The Following PlainText You Would Like To Encrypt:
tellhimaboutme

Please Choose From The Following Options:
1 - Encrypt Using Manual Encryption
2 - Encrypt Using Preloaded Key
2
Encrypting the Following Text:
tellhimaboutme
Encrypted Message:
VEQPJIREDOZXOE
```

6. If you enter option 2, you can manually select the key you would like to implement for the vigenere cipher.

7. After finishing the Encryption, we go back to the main menu and select Bob's view where we will already have either the preloaded key or the updated key from Alice's view to Decrypt. Bob's view as follows:

```
Bob's View
Here You Will Be Able To Decrypt Any CipherText.
Enter The Following CipherText You Would Like To Decrypt:
veqpjiredozxoe
Decrypting The Following Text:
veqpjiredozxoe
Decryption:
TELLHIMABOUTME

Please Choose From The Following Options:
1 - Alice's View
2 - Bob's View
3 - Eve's View
4 - Exit The Program
```

8. Let's say we used a manual key "abc" it would follow as:

```
Alice's View:

Here You Will Be Able To Encrypt Any PlainText.
Enter The Following PlainText You Would Like To Encrypt:
tellhimaboutme

Please Choose From The Following Options:
1 - Encrypt Using Manual Encryption
2 - Encrypt Using Preloaded Key
1

Enter The Manual Key You Would Like To Use For Encryption.
Please Do Not Use Spaces
abc
TFNLIKMBDOVVMF

Please Choose From The Following Options:
1 - Alice's View
2 - Bob's View
3 - Eve's View
4 - Exit The Program
2

Bob's View
Here You Will Be Able To Decrypt Any CipherText.
Enter The Following CipherText You Would Like To Decrypt:
TFNLIKMBDOVVMF
Decrypting The Following Text:
TFNLIKMBDOVVMF
Decryption:
TELLHIMABOUTME
```

9. Looking at Eve's View:

Here We Have the Variances From the Original CipherText and the Occurrences for the CipherText.

```
Letter Occurrences for Cipher Text:
A = 253.0
B = 103.0
C = 232.0
D = 142.0
E = 481.0
F = 312.0
G = 389.0
H = 310.0
I = 559.0
J = 481.0
K = 262.0
L = 222.0
M = 321.0
N = 407.0
O = 248.0
P = 236.0
Q = 278.0
R = 364.0
S = 492.0
T = 496.0
U = 252.0
V = 347.0
W = 403.0
X = 364.0
Y = 338.0
Z = 67.0
```

```
Letter Frequencies of CipherText:
A = 0.030266778322765 88
B = 0.012322048091877019
C = 0.02775451609044144
D = 0.01698767795190812
E = 0.05754276827371695
F = 0.03732503888024884
G = 0.04653666706543845
H = 0.03708577581050365
I = 0.06687402799377916
J = 0.05754276827371695
K = 0.03134346213661921
L = 0.026558200741715516
M = 0.038401722694102164
N = 0.04869003469314511
O = 0.029668620648402918
P = 0.02823304222993181
Q = 0.033257566694580694
R = 0.04354587869362364
S = 0.058858715157315465
T = 0.059337241296805836
U = 0.03014714678789329
V = 0.041512142600789566
W = 0.04821150855365474
X = 0.04354587869362364
Y = 0.04043545878693624
Z = 0.008015312836463692
```

10. Here We Have the Variances From the Original Plain Text and the Occurrences for the Plain Text.

```
Letter Occurrences For PlainText (EVE CANNOT ACCESS THIS):
A = 593.0
B = 123.0
C = 230.0
D = 348.0
E = 1101.0
F = 196.0
G = 139.0
H = 459.0
I = 657.0
J = 28.0
K = 53.0
L = 291.0
M = 159.0
N = 563.0
O = 681.0
P = 144.0
Q = 5.0
R = 518.0
S = 674.0
T = 773.0
U = 219.0
V = 65.0
W = 196.0
X = 22.0
Y = 119.0
Z = 3.0
```

```
Letter Frequencies of PlainText (NOT WHAT YOU CAN SEE IN EVE'S VIEW):
A = 0.07094150017944731
B = 0.014714678789328866
C = 0.027515253020696257
D = 0.04163177413566216
E = 0.13171431989472424
F = 0.023447780835028114
G = 0.016628783347290347
H = 0.05491087450651992
I = 0.07859791841129321
J = 0.0033496829764325877
K = 0.006340471348247398
L = 0.03481277664792439
M = 0.019021414044742193
N = 0.06735255413326953
O = 0.08146907524823543
P = 0.017226941021653307
Q = 5.98157674362962E-4
R = 0.061969135064002874
S = 0.08063165450412729
T = 0.09247517645651394
U = 0.026199306137097738
V = 0.007776049766718507
W = 0.023447780835028114
X = 0.002631893767197033
Y = 0.014236152649838497
Z = 3.5889460461777724E-4
```

11. From this, we can tell that none of the frequencies from the plaintext matches the frequencies from the ciphertext. What does this mean? When we go back to the substitution cipher, Eve was able to decrypt the corpus because each letter was assigned to another letter and it was a one-to-one ratio. So if letter "A" from the entire corpus occurred 13.42% and "A" was paired to letter "Z", Z would occur 13.42% times within the ciphertext. Let's run Eve's view one more time:

(Continues On Next Page)

12. Eve Running another time using different key (Key: COOKIES):

```
Letter Occurrences For PlainText
A = 593.0
B = 123.0
C = 230.0
D = 348.0
E = 1101.0
F = 196.0
G = 139.0
H = 459.0
I = 657.0
J = 28.0
K = 53.0
L = 291.0
M = 159.0
N = 563.0
O = 681.0
P = 144.0
Q = 5.0
R = 518.0
S = 674.0
T = 773.0
U = 219.0
V = 65.0
W = 196.0
X = 22.0
Y = 119.0
Z = 3.0

Letter Frequencies of PlainText
A = 0.07094150017944731
B = 0.014714678789328866
C = 0.027515253020696257
D = 0.04163177413566216
E = 0.13171431989472424
F = 0.023447780835028114
G = 0.016628783347290347
H = 0.05491087450651992
I = 0.07859791841129321
J = 0.0033496829764325877
K = 0.006340471348247398
L = 0.03481277664792439
M = 0.019021414044742193
N = 0.06735255413326953
O = 0.08146907524823543
P = 0.017226941021653307
Q = 5.98157674362962E-4
R = 0.061969135064002874
S = 0.08063165450412729
T = 0.09247517645651394
U = 0.026199306137097738
V = 0.007776049766718507
W = 0.023447780835028114
X = 0.002631893767197033
Y = 0.014236152649838497
Z = 3.5889460461777724E-4
```

```
Letter Occurrences for Cipher Text:
A = 301.0
B = 339.0
C = 416.0
D = 225.0
E = 196.0
F = 329.0
G = 540.0
H = 339.0
I = 323.0
J = 172.0
K = 405.0
L = 235.0
M = 359.0
N = 127.0
O = 405.0
P = 266.0
Q = 315.0
R = 284.0
S = 613.0
T = 202.0
U = 193.0
V = 498.0
W = 566.0
X = 263.0
Y = 194.0
Z = 254.0

Letter Frequencies of CipherText:
A = 0.03600909199665032
B = 0.04055509032180883
C = 0.049766718506998445
D = 0.026917095346333294
E = 0.023447780835028114
F = 0.039358774973082905
G = 0.0646010288311999
H = 0.04055509032180883
I = 0.03864098576384735
J = 0.020576623998085894
K = 0.048450771623399926
L = 0.028113410695059217
M = 0.04294772101926068
N = 0.015193204928819237
O = 0.048450771623399926
P = 0.03182198827610958
Q = 0.03768393348486661
R = 0.03397535590381624
S = 0.07333413087689915
T = 0.024165570044263666
U = 0.023088886230410336
V = 0.05957650436655102
W = 0.0677114487378873
X = 0.031463093671491804
Y = 0.02320851776528293
Z = 0.030386409857638474
```

13. As we can see there is no pattern in terms of frequencies of letters that Eve can use. The purpose of a vigenere cipher is to encrypt data in such a way that frequencies of letters from a ciphertext cannot be matched to occurrences of a letter from a corpus. The substitution cipher allows people like Eve to use these frequencies to decrypt the corpus and ultimately break down our key. From the Vigenere Cipher, there exist no frequency patterns, thus Eve cannot use frequencies to obtain the code for our encryption. As a result, the vigenere cipher makes our plaintext exponentially harder to breach. No matter how many times you run the program and how long a corpus is, Eve will not be able to use a frequency analysis to breach our encryption.