

Lab 03 - Vigenere Cipher

1) List the five most common trigrams

(10 total points. 2 points each)

- "BKM"
- "GHM"
- "THB"
- "YEB"
- "WPR"

2) Show the difference between the starting indexes of the five most common trigrams.

(10 total points, 2 points each)

- "BKM" positions = [205, 50, 15, 125, 150, 80, 70, 275]
- "GHM" positions = [90, 290, 385, 35, 105]
- "THB" positions = [105, 35, 253, 72, 220]
- "YEB" positions = [85, 35, 65, 230, 30]
- "WPR" positions = [95, 185, 350, 10]

3) Based on your findings, what do you suspect the key length is? Justify your answer.

(10 total points, 5 points length value, 5 points justification)

- 5, because it is the most common factor out of the differences included from each index.

4) Separate the ciphertext into X shift-by-N ciphers where X is the length of the key and perform monoalphabetic frequency analysis on each. What are the three most common ciphertext characters in each of the shift-by-N ciphers?

(20 total points, 10 points for separating into X shift-by-N ciphers, 10 points for the common ciphertext characters in each shift-by-N cipher.)

- "BKM" = [b, w, m]
- "GHM" = [h, w, q]
- "THB" = [m, b, i]
- "YEB" = [r, v, a]
- "WPR" = [t, e, o]

5) Decrypt the ciphertext using the potential key values you found in question 5. Show all iterations, the final keyword, and the final plaintext.

(25 total points, 15 points for all iterations, 5 points for correct keyword, 5 points for correct plaintext)

```
Enter character 0 (likely to be in the keyword): l
///////// Cipher 4 Potential Key Values ///////////

Most frequently occurring ciphertext characters from left to right:
['i', 't', 'd', 'c', 'h', 'p', 'w', 'x', 'g', 'a', 's', 'r', 'b', 'z', 'v', 'j',
 'l', 'n', 'e', 'k', 'u', 'o', 'f', 'm', 'q', 'y']

Most likely 5 character(s) in the keyword: ['i']
```

```
Enter character 1 (likely to be in the keyword): q
///////// Cipher 4 Potential Key Values ///////////

Most frequently occurring ciphertext characters from left to right:
['d', 'o', 'y', 'x', 'c', 'k', 'r', 's', 'b', 'n', 'v', 'm', 'u', 'w', 'q', 'e',
 'g', 'i', 'f', 'p', 'z', 'j', 'a', 'h', 'l', 't']

Most likely 5 character(s) in the keyword: ['d']
```

```
Enter character 2 (likely to be in the keyword): l
///////// Cipher 4 Potential Key Values ///////////

Most frequently occurring ciphertext characters from left to right:
['i', 't', 'd', 'c', 'h', 'p', 'w', 'x', 'g', 'a', 's', 'r', 'b', 'z', 'v', 'j',
 'l', 'n', 'e', 'k', 'u', 'o', 'f', 'm', 'q', 'y']

Most likely 5 character(s) in the keyword: ['i']
```

```
Enter character 3 (likely to be in the keyword): g
///////// Cipher 4 Potential Key Values ///////////

Most frequently occurring ciphertext characters from left to right:
['n', 'y', 'i', 'h', 'b', 'c', 'm', 'u', 'l', 'f', 'x', 'w', 'e', 'g', 'a', 'o',
 'q', 's', 'j', 'p', 'z', 't', 'd', 'k', 'r', 'v']

Most likely 5 character(s) in the keyword: ['n']
```

```
Enter character 4 (likely to be in the keyword): t
///////// Cipher 4 Potential Key Values ///////////

Most frequently occurring ciphertext characters from left to right:
['a', 'l', 'v', 'u', 'h', 'o', 'p', 'z', 'y', 'k', 's', 'j', 'r', 't', 'n', 'b',
 'd', 'f', 'c', 'm', 'w', 'g', 'e', 'i', 'q', 'x']

Most likely 5 character(s) in the keyword: ['a']
```

```
////////// Plaintext using the key: idina //////////
```

```
thesnowglowswhiteonthemountaintonightnotafootprinttobeseenakingdomofisolationa  
nditlookslikeimthequeen  
thewindishowlinglikethisswirlingstorminsidecouldntkeepi  
tinheavenknowsitrieddontletthemindontletthemseebethegoodgirlyoualwayshavetobec  
oncealdontfeeldontletthemknowwellnowtheyknowletitgoletitgocantholditbackanymor  
eletitgoletitgoturnawayandslamthedoordontcarewhattheyregoingtosayletthestorm  
rageonthe cold never bothered me anyway its funny how some distance makes everything seem sma  
ll and the fears that once controlled me cant get to me eat all it stims to see what i can do to test t  
he limits and break through no right now wrong no rules for me i m free let it go let it go i am onewit  
h the wind and sky let it go let it go you ll never see me cry here i stand and here i stay let the stor  
m rage on my power flurries through the air into the ground my soul is spiraling in frozen fract  
als all around and onethought crystallizes like a icy blast i m never going back the past is in  
the past let it go let it go and ill rise like the break of dawn let it go let it go that perfect girl  
is gone here i stand in the light of day let the storm rage on the cold never bothered me anyway
```

6) Submit your documented python code on canvas.

(25 total points, 10 points for documentation, 15 points for working code. No points awarded if the code is copy/pasted from someone else.)