

ISC 1057 – Homework # 4

Fall 2017

Assigned: 9/26/17

Due: 10/5/17

1. In this problem we want to encrypt the message

CEASE FIRE AT ELEVEN

using a Vigenere Cipher where the key is the word **DOG**.

- (a) First, determine what position each letter of the key word DOG is in the alphabet.

- (b) Break the message into 3 letter blocks and write the correct number of shifts below each letter Next, shift each letter by the indicated amount to get the encrypted message.

C E A S E F I R E A T E L E V E N

2. In this problem we want to use frequency analysis to decrypt a longer message which was encrypted using a monoalphabetic substitution cipher. It is a quote and the encrypted quote is given on the next page.

(a) Complete the frequency table for the letters occurring in the message.

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

- (b) Use PLOTLY (or another plotting program that you are familiar with) to make a frequency bar plot of your results in (a). The x -axis should be the letters of the alphabet and the y -axis the number of times that letter occurs in the message.
- (c) Complete the table below indicating the short encrypted words (containing 1-4 letters) in the message and in parentheses indicate the number of times that the word appears.

1-letter words:

2-letter words:

3-letter words:

4-letter words:

- (d) Use your results from (a) - (c) to decrypt 10 letters in the message. Record your results below and give your reasoning. If you try something and it doesn't work, indicate why. Show your work on the next page. Hint: "B" encrypts an "E".

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

- (e) For extra credit, decrypt the entire message. You must give the reasoning for each choice.

Points: # 1 - 10pts # 2a -8 pts, 2b- 4 pts, 2c - 8pts, 2d- 20 pts 2e- 10pts (extra credit)

\overline{V} \overline{P} \overline{B} \overline{V} \overline{T} \overline{M} \overline{W} \overline{L} \overline{D} \overline{B} \overline{I} \overline{A} \overline{V} \overline{P}

\overline{P} \overline{Q} \overline{N} \overline{A} \overline{S} \overline{Y} \overline{Q} \overline{S} \overline{M} \overline{F} \overline{B} \overline{S} \overline{O} \overline{A} \overline{S} \overline{J}

\overline{A} \overline{H} \overline{V} \overline{P} \overline{Q} \overline{V} \overline{F} \overline{B} \overline{M} \overline{F} \overline{D} \overline{B} \overline{I} \overline{A} \overline{D} \overline{D}

\overline{A} \overline{S} \overline{H} \overline{A} \overline{H} \overline{V} \overline{M} \overline{S} \overline{V} \overline{T} \overline{U} \overline{A} \overline{S} \overline{Y} \overline{V} \overline{M}

\overline{F} \overline{W} \overline{V} \overline{V} \overline{P} \overline{A} \overline{S} \overline{Y} \overline{H} \overline{A} \overline{S} \overline{A} \overline{V}