POLYALPHABETIC CIPHERS: CODE WORD CIPHERS

We saw that with shift ciphers, a simple frequency analysis can reveal the shift quite easily. If we use multiple shifts we can complicate the problem slightly. In this cipher, we will encrypt using a CODE WORD. The code word is written repeatedly over the top of the plaintext and added (mod 26) to get the cipher text. We will use direct numerical substitution to replace letters.

(NOTE: For this worksheet only we have A=1, Z=26 so refer to the following table only when working on this worksheet.)

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

EXAMPLE:

```
      Key:        K EYKE YK EYKEYKE YKEYKEYK
Plaintext:        I LIKE TO ENCRYPT MESSAGES.
Ciphertext:       T QHVJ…..
```

K+I = 11+9 = 20 = T
E+L = 5+12=17=Q
Y+I = 25+9=34=8=H
ETC.

3. The following ciphertext was created using the code word MATH. *Decipher* the code to find the hidden message.

N C M B E B W D N M A M O S U Q F G O V

4. Notice that the two I's in the plaintext in example 2 have different ciphertext (the first encodes to a T, the second encodes to an H): different letters in the cipher text may both correspond to the same letter. Also notice that the 2 B's in the ciphertext in example 3 did not decrypt to the same letter. So you can't do a simple frequency analysis to figure out they key. Assuming you can guess the length of the key, how could you do a frequency analysis on ciphertext that has been encrypted with a code word to figure out the key?

5. Try your method on the following ciphertext to see if you can figure out the codeword. The length of the codeword is 3. (Hint: the next page may help.)

CIPHERTEXT

C D B T D S Z C S V J C N N T X D S T Y S K T C X Z S

G O G K B U Y Z J K M M K Q S T D B M J F K G G K C S

K V H Y K S G N O T Y D K V F Y W I Z C S T Z J K M B

K Z R Y O C Y V M V G S G N S

Math 440

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

Math 440

Math 440