Math Circle - Spring 2012 - Homework 7

1. (10 points) The following is a block of text on which a substitution cipher has been performed. That is, each letter of the alphabet has been replaced by some other letter. Determine what the original text said.

NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV KAS NOTES OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS AK NOT KMWEJX UMZ UENO NOTW, AL NOT NOTASX NOMN ZOT UACJP QTTY NOT GEZENASZ ADDCYETP PCSELV NOT UMEN.

NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, KSTDQTJP, RCDQ NAANOTP MLP RTZYTDNMDJTP. ZOT WMELNMELTP M PTTY ZEJTLDT MLP NOT NUA JMPETZ YTTSTP PACRNKCJJX MN OTS.

KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS, ‘‘LAN GTSX Y-S-T-N-N-X, E KTMS,’’ DMSTKCJJX ZYTJJELV NOT QTX UASP.

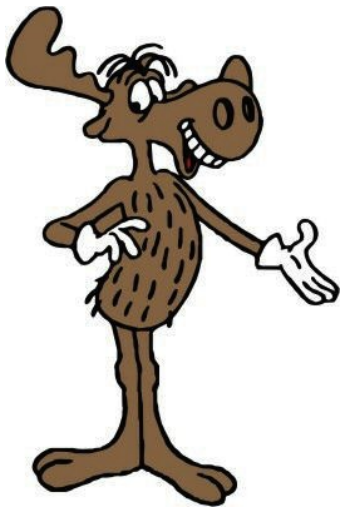
UOTSTCYAL NOT DOEJP YEYTP CY, ‘‘RCN MUKCJ Z-W-M-S-N!’’

In case you want to use it, here is a table telling you how often each letter appears in the above block.

A	B	C	D	E	F	G	H	I	J	K	L	M
25	0	14	10	28	0	3	0	1	23	10	18	25

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
44	31	24	4	5	22	60	14	7	7	11	13	23

2. (5+5+5 points) Rocky has a secret message $\mathscr{M}$ which he wants to send to Bullwinkle. This message is some block of text. Rocky needs to encrypt the message so that Boris cannot understand it if he intercepts it. He decides that the best way to encrypt is to perform some substitution cipher on the message $\mathscr{M}$.



For an added layer of security, Rocky actually creates two substitution ciphers E and E'. Both ciphers somehow swap around all 26 letters of the alphabet. Rocky first creates a new message $E(\mathscr{M})$ by applying the cipher E to his message. *THEN* Rocky decides to even further encrypt this new message by applying the cipher E' to the letters of the encrypted message $E(\mathscr{M})$. He then sends Bullwinkle the completely encrypted $E'(E(\mathscr{M}))$.

(a) Has Rocky actually added a new layer of security by encrypting the message twice? Why or why not?

(b) Determine two substitution ciphers E and E' such that if Rocky encrypts in the opposite order, he wil get a different result: that is, $E'(E(\mathscr{M})) \neq E(E'(\mathscr{M}))$.

(c) Bullwinkle can decrypt the cipher E by applying the "inverse cipher" D. In symbols, this means $D(E(\mathscr{M})) = \mathscr{M}$. He can similarly decrypt E' with D'. How will Bullwinkle be able to decrypt Rocky's doubly-encoded message $E'(E(\mathscr{M}))$?

3. (5 points) As in Problem 2 above, Rocky has a secret block of text which he wants to encrypt and then send to Bullwinkle. Rocky decides to treat each of the 26 letters of the alphabet as numbers ($A = 1$, $B = 2$, $\ldots$, $Z = 26$). In order to encrypt his message, Rocky picks some random integer ξ between 1 and 26, then multiplies each letter by ξ and reduces modulo 27 to get the encrypted version.

For example, if $\xi = 7$ and the message is DOG, the encrypted message is AXV:

Letter	**Value**	**Multiply by ξ**	**Modulo 27**	**New Letter**
D	4	28	1	A
O	15	105	24	X
G	7	49	22	V

Do you think that in general this is a good encryption method for Rocky? Why or why not? *Hint.* Don't forget about Bullwinkle!