POLYALPHABETIC CIPHERS

MTH 440

Monoalphabetic ciphers

- Our examples of the permutation, shift, decimation, and affine ciphers were *monoalphabetic* ciphers, that is every letter was replaced by the same letter each time.

- H**v** ufe fh <u>kar</u> <u>kar</u>**v**edrh **v**u pf<u>ka</u>rpfkdlh fer fi**v**nk erfmdkz, <u>kar</u>z fer s**v**k Irekfds; h**v** ufe fh <u>kar</u>z fer Irekfds, <u>kar</u>z fer s**v**k fi**v**nk erfmdkz. – Fmirek Rdshkrds.

- In a decimation cipher A always represents itself

- Even a random substitution cipher with 26! ~ 4 x 10^{26} different possible "keys" is easy to solve with a simple frequency analysis (given enough ciphertext)

Polyalphabetic ciphers

- In a polyalphabetic cipher, multiple "alphabets" are used to encipher.
- If two letters are the same in the ciphertext it does not mean they must decipher to the same plaintext letter.

Vigenere cipher - codeword

KEY: K E Y K E Y E
PLAIN: T R Y T H I S
            D

Vigenere Cipher - codeword

KEY: K E Y K E Y E
PLAIN: T R Y T H I S

D

D V W D L G W

Finish enciphering (problem 1)

Vigenere - decipher

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

KEY: K E Y

Cipherext D A M

T

T W O

Finish deciphering (problem 2)

Polyalphabetic ciphers

BYIRL BFMVG SXFEJ FJLXA MSVZI QHENK FIFCY JJRIF SEXRV CICDT EITHC BQVXS GWEXF PZHHT JGSPL HUHRP FDBPX NLMFV TFMIG RBZJT XIGHT JDAMW VMSFX LHFMS UXSDG EZDIE PCZLK LISCI JIWSI HTJVE VWVFM VWISO DFKIE QRQVL EPVHM YZSRW CIMZG LWVQQ RAWRT ZFKYV HOZIF JRDHG WVWKR RQSKM XOSFM VQEGS OJEXV HGBJT XXRHT JFTMQ WASJS JPOZP ZRHUS CZZVI VHTFK XLHME MFYPG RQHCE VHHTJ TEYVS EBYMG KWYUV PXKSY YFXLH GQURV EWWAS

The frequency analysis of a polyalphabetic cipher looks different than plaintext or monoalphabetic analyses. Which is which?
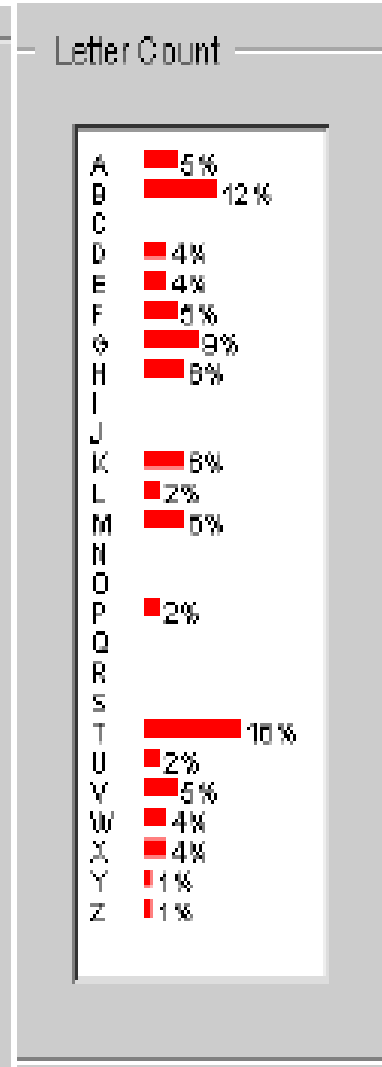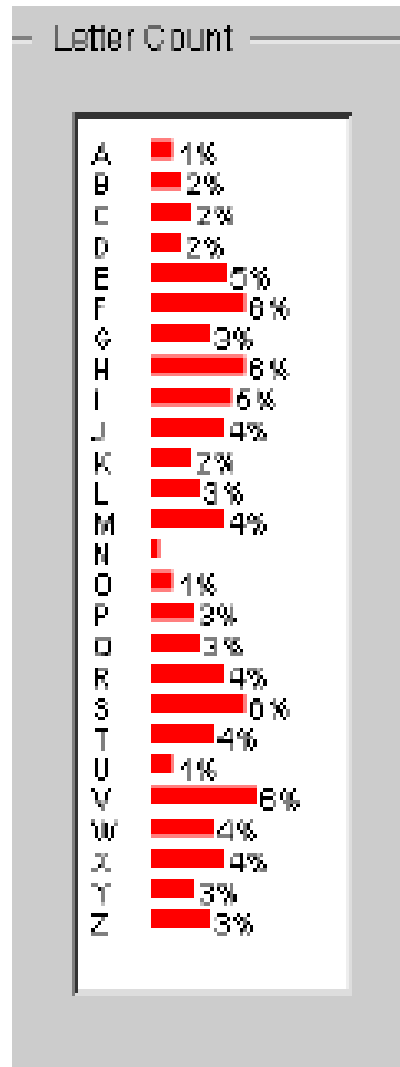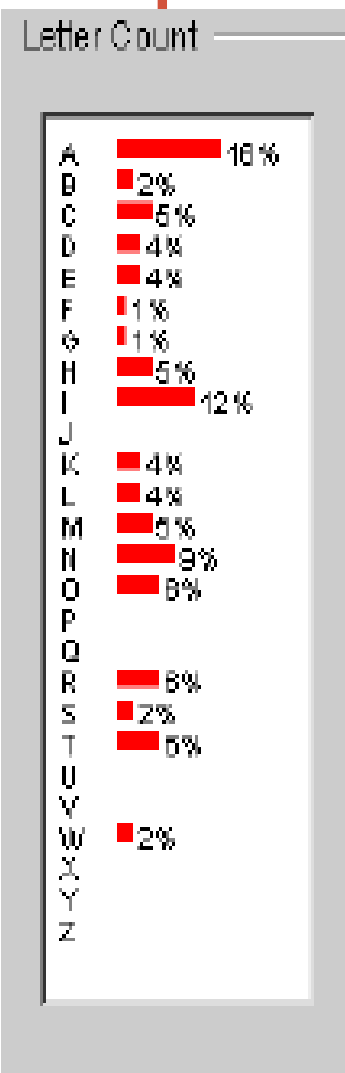
Breaking a polyalphabetic

jprwsttiqrugmyzfnvhcnscffnyjufybnqznubvqiftjujlnsxrayedab
txcmcytmbubrwcffnyjufybnqznrugmyzfnvhcnszenyqwcpmz
ejar

Hint code length 3

jprwsttiqrugmyzfnvhcnscffnyjufybnqznubvqiftjujlnsxrayedab
txcmcytmbubrwcffnyjufybnqznrugmyzfnvhcnszenyqwcpmz
ejar

Breaking a polyalphabetic

jprwsttiqrugmyzfnvhcnscffnyjufybnqznubvqiftjujl
nsxrayedabtxcmcytmbubrwcffnyjufybnqznrugmy
zfnvhcnszenyqwcpmzejar

jwtrmfhsfjyquqtjsadtmtuwfjyqrmfhsnwmj
Most frequent: j

psiuynccnubzbijlxyaxcmbcnubzuynczycza
Most frequent: c

rtqgzvnfyfnnvfunrebcybrfyfnngzvneqper
Most frequent: n

Possible codewords

- The most common English letters are
- E T A O I N S H R

	E	T	A	O	I	N	S
J	F	Q	J				
C	Y						
N	J						

- Finish filling out the chart
- Try to make a word
- Check your guess by trying to decipher (problem 3)

http://rumkin.com/tools/cipher/vigenere-keyed.php

What if you don't know the codeword length?

- jprwsttiqrugmyz<u>fn</u>vhcnscf<u>fn</u>yjufybnqznubvqiftjujlnsxrayeda
btxcmcytmbubrwcf<u>fn</u>yjufybnqznrugmyz<u>fn</u>vhcnszenyqwcp
mzejar

- The fn pairs are separated by 9, 48, and 18 suggesting the codeword length is a common factor.

Vigenere with crib

Cipher Challenge 2:

The following ciphertext is believed to have been enciphered quickly using the Vigenére method. We believe the coded message refers to an individual whose codename is JITTERBUG and, most importantly, we know that the message indicates a time and place for an upcoming meeting. We know the city in which the meeting is to take place, but we lack the specific details of when and where this meeting will occur. Other trustworthy sources have indicated that part of the message might refer to a recent incident which took place in Cataluna, Spain. Obviously, spacing and word lengths have not been preserved during the encryption process. Again, we desperately need to know the exact time and place of the meeting in order to apprehend these enemy agents. Time is of the essence on this one.

```
ZEGXV  NDXMU  BKZJY  YMTUS  HTGAT  RMIHV
                            JITTE  RBUG

CVYOL  IFRAQ  HGFIA  ENGZK  YYXAV  XPXFO
              JITTE  RBUG

FKKPZ  XQSGT  WVQMJ  VOGLP  CONIE  JUTVO
                                  JITTE  RBUG
```