Fun with Ciphers

September 26, 2010

0.1 Monoalphabetic (Substitution) ciphers

- A "monoalphabetic" cipher means that the same cipher alphabet is used throughout the substitution.
- To encode a message with this kind of cipher, replace the "Original" letter with the "Encoded" letter from the key.
- To decode a message, do the opposite: replace the "Encoded" letter with its corresponding "Original" from the key.

1. Consider one example of a key for a monoalphabetic cipher

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

   (a) Do you see a pattern in how this key is organized?

(b) Use the key on the previous page to decode the message below:

FXOZNZGSXRIXOV

(c) Create your own monoalphabetic cipher key below

(Remember to only use each letter once in the "Substitute" row)

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

i. Use the key to encode a message and pass it over to your partner to decode.
Encoded message:

Decoded message (let your partner decode):

0.2 Caeser cipher

The simplest of monoalphabetic ciphers is the *Caesar (or shift) cipher.*
In this cipher, the key is just a "shifted" alphabet.

1. This is an example of a Caesar cipher

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

Notice that the end of the alphabet "wraps around" to the beginning, so when we reach the end of the alphabet, we begin again.

The shift of this cipher is "+4." Each letter in the original text is replaced by the letter which comes 4 after it.

(a) Use the key above to encode your name:

(b) Let your partner decode:

(c) Fill in the key for a Caesar cipher with a shift of +7:

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

Use your key above to decode the following message:

FVBCLNVAPA

0.3 Using Frequency of Letters to Decode

1. Knowing how frequently various letters of the alphabet are used in a text can help one decode an en encryption. What letter(s) do you think are encountered most often in a long text? Make a guess (or several guesses)

2. Below is the graph showing how often certain letters occur in typical English language text

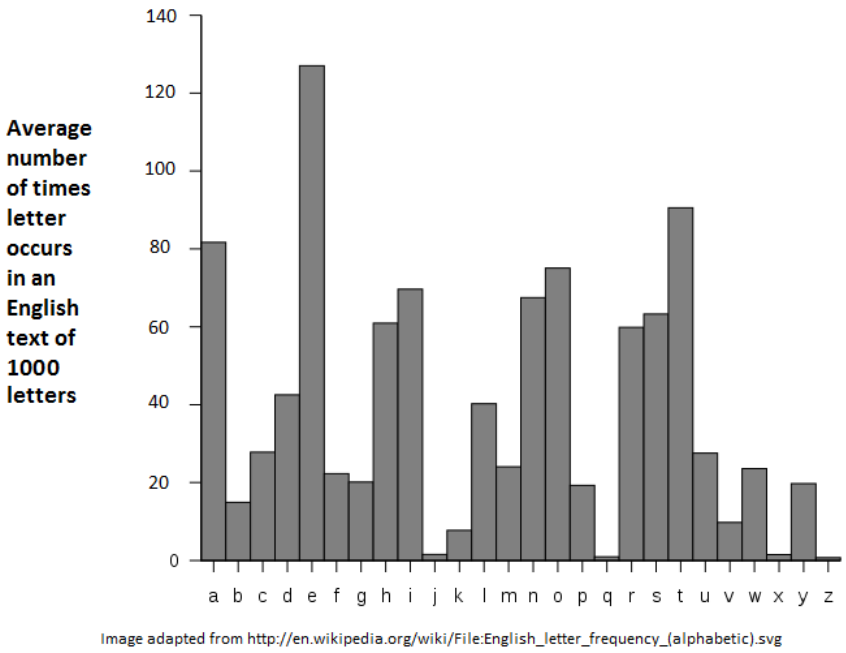

Image adapted from http://en.wikipedia.org/wiki/File:English_letter_frequency_(alphabetic).svg

   (a) How can we use this graph to analyze a shift or other substitution cipher?

(b) Cara received an encrypted message that was a thousand letters long. She counted up how many times each letter occurred in the text. Below are the top 5 occurring letters. Use the graph above to try to match the encoded letter to the letter it is substituting from the original text

Encoded Letter	How many?	Decoded Letter
G	127	
M	91	
P	82	
L	75	
R	70	

(c) Do you think the frequency method would work for short messages (e.g., 50 letters)? Why or why not?

3. Count up how many times each letter occurs in the following message:

KFOBICOMBODWOCCKQO

Letter:	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
# in text:									
Letter:	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
# in text:									
Letter:	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	-
# in text:									-

(a) What letter occurs most often?

(b) If we match that letter with E in a shift (Caeser) cipher, what is the shift?

(c) Use your cipher wheel to decode the secret message from the previous page:

KFOBICOMBODWOCCKQO

(d) Without knowing that this a shift cipher, would you still be able to decode as quickly? Why or why not?

0.4 Pigpen cipher

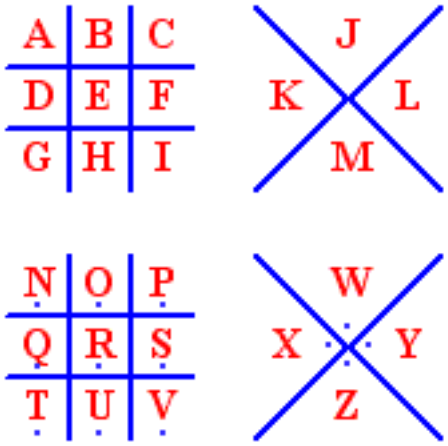

Image adapted from:
http://www.borderschess.org/Freemason.gif

1. Encode the following message using Pigpen cipher
   ENCRYPTION

2. Write your own message to your partner using this cipher, and see if they can decode it!

   Encoded message:

   Decoded message:

0.5 Rail Fence Cipher

Here is how we can encode the phrase WHO GOES THERE using the Rail Fence cipher

- First, make an outline of the zig-zag pattern for the number of letters that are in your message
  (WHO GOES THERE has 12 letters)

_				_				_			
	_		_		_		_		_		_
		_				_				_	

- Arrange the letters a zig-zag pattern on three lines:

W				O				H			
	H		G		E		T		E		E
		O				S				R	

- Then, the encoded phrase is written out left-to-right, top-to-bottom:

WOHHGETEEOSR

1. Use the Rail Fence cipher to encode the message

I WILL BE THERE SOON

_				_				_				_		_	
	_		_		_		_		_		_		_		_
		_				_				_				_	

(a) What will the encoded text read?

2. Decoding Rail Fence cipher

(a) The algorithm:

i. Count the number of letters in the message.

ii. Make an outline of the zig-zag pattern like we did in the example above for the number of letters in the message

A. Fill in the top row first

B. Then fill in the middle row

C. Finally, fill in the third row

iii. Read the message, inserting spaces where necessary

(b) Decode the following message that was encoded with the Rail Fence cipher:

IEHTLVMTEAISOAMC

i. How many letters are in the message?

ii. Fill in the decoding outline below:

_				_				_				_			
	_		_		_		_		_		_		_		_
		_				_				_				_	

iii. Write out the original message below:

3. (Challenge problem)
   The following message was written using a (non-Caesar) monoalphabetic substitution cipher. Look at the structure. Can you decode the message?

   TULS CKMTUOKC,

   BUANEWU RLNH!

   -CDLOOEO

Homework

- Learn about one more cipher, or design one of your own. Come next week with a message encrypted with that cipher and a key to decode it.