More Fun with Ciphers

October 3, 2010

1 Using frequencies to decode

Image adapted from http://en.wikipedia.org/wiki/File:English_letter_frequency_(alphabetic).svg
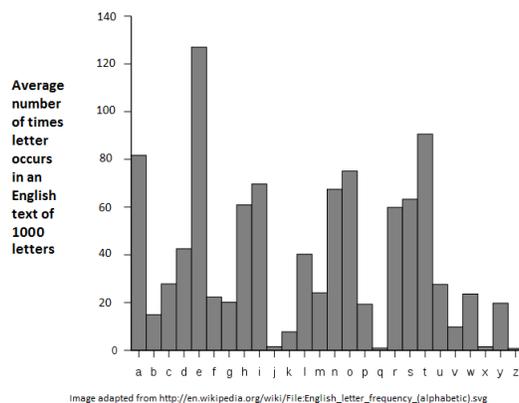
1. Daniel received an encoded message of 1000 characters. He counted up how often every letter occurred and listed the top 5 most frequent letters below. Use the graph to match the letters that occur most often in the encoded message to the original letters.

Substitution Letter	# of times	Original letter
R	127	
S	90	
D	81	
E	76	
A	70	
Q	66	
T	63	
C	60	

(a) Copy the table from the previous page here:

Substitution Letter	# of times	Original letter
R	127	
S	90	
D	81	
E	76	
A	70	
Q	66	
T	63	
C	60	

(b) Below is a sample of some text from the message that Daniel received. Decode the message by first replacing the letters you found above into the text. Then, see if you can figure out what the rest of the message reads.

A MEHQP SCR RQRYI CAPREHS.


AS AT BRCAQP SCR ELP SZRR.

2 Pigpen cipher

Image adapted from:
http://www.borderschess.org/Freemason.gif
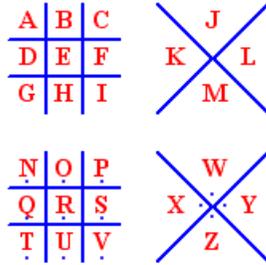
1. Encode the following message using Pigpen cipher:

   SYMBOLS

2. Decode this message written using the Pigpen cipher:

3. Encode your own message using the Pigpen cipher, and pass it to your partner to decode:
   Encoded message:

   Decoded:

3 Rail Fence Cipher

1. Encoding the Rail Fence Cipher

   (a) Here is how we can encode the phrase WE ARRIVE SOON using the Rail Fence cipher

      i. First, make an outline of the zig-zag pattern for the number of letters that are in your message
      (WE ARRIVE SOON has 12 letters)

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

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

W				R				S			
	E		R		I		E		O		N
		A				V				O	

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

WRSERIEONAVO

   (b) Use the Rail Fence cipher to encode the message

MATH IS GREAT

_				_				_		
	_		_		_		_		_	
		_				_				_

      i. 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:

   # RFEHALECCPEINIR

      i. How many letters are there in the message?

      ii. Fill in the decoding outline below:

| _				_			_		_	
	_		_		_		_		_	
		_			_			_		_

      iii. Write out the original message below:

4 Cardan Grille

In this method of encoding, a message is hidden within other text, and the key to decoding it is a grid with cutouts that reveal the letters of the actual message.

1. Below is a message that appears to be a letter from someone named Alice to her Cousin Ralph. After looking at it using the attached grid, it reveals a hidden message.

Cousin Ralph,
I hope you are doing well, as always. I was quite impressed by the pictures you sent, thank you. Hopefully we will see you soon.
-Alice
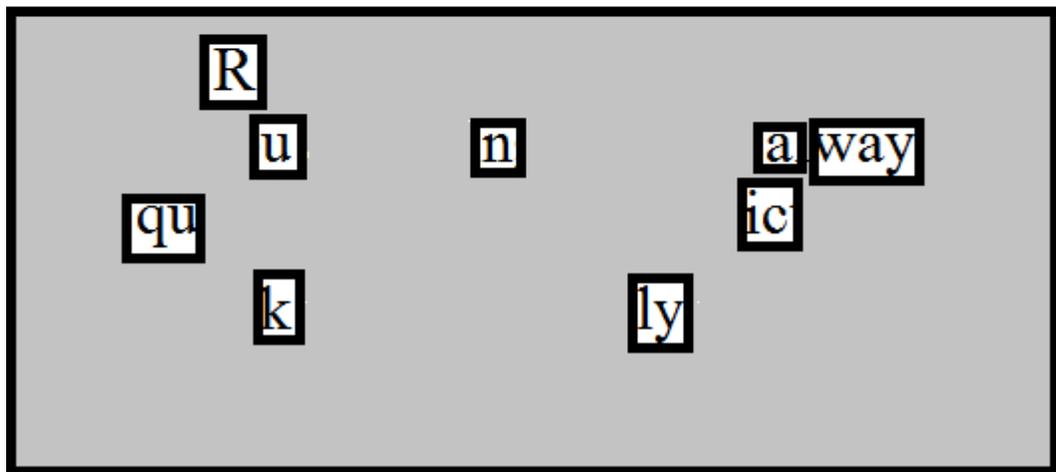
What is this letter really telling the reader?

2. Sometimes the message is hidden within other words. Use the grille at your table to decode the message hidden in the words below:

W	H	E	N
W	I	L	L
L	A	N	D
H	A	L	O

3. Notice that the surrounding letters do not need to be really meaningful. Find the message in the text below using your grille again.

D	A	P	N
W	T	R	L
P	L	X	D
Q	U	L	E

4. Use the tables below, and the grille at your table, to encode your own secret messages, then pass it to your partner to decode:

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

Decoded messages:

5 Hidden information in account numbers [1]

Did you know that bank and credit card accounts hold information even in the numbers of the accounts? Certain credit card companies set the account numbers up so it is easy to verify that the number belongs to a real card. The "Circle Credit Company" issues credit cards whose number can be verified as follows:

- First, compute a certain *Value* associated to the card;

- Second, check if this *Value* is a number that ends with a 0.

  - Cards whose numbers have an *Value* that ends with the digit 0 are likely *Circle Credit* cards.
  - If the *Value* ends with any digit other than 0 , the number we started with is not a number of an actual credit card.

For example, let's check if a card whose number appears below can be an actual card issued by the *Circle Credit Company*:

4316 9940 1203 9603

1. First we compute the *Value* following certain rules.

   (a) Beginning with the digit in the right-most position, write down *every other* digit underneath its original position. (Do not write anything below the digits in the even-numbered positions.)

4316 9940 1203 9603

4	3	1	6	9	9	4	0	1	2	0	3	9	6	0	3

(b) Then, for the digits that have nothing written underneath them, add the digit to itself.

  i. If the result is a one digit number, write it below the digit you started with;

  ii. If the result is a two digit number, add these two digits and write the result below the digit you started with.

Example 1: if the digit is 3, add $3 + 3 = 6$, and write 6 under 3.
Example 2: if the digit is 7, add $7 + 7 = 14$, add $1 + 4 = 5$, and write 5 under 7.

Now, do it for all the digits of the number we are checking:

4316 9940 1203 9603

4	3	1	6	9	9	4	0	1	2	0	3	9	6	0	3
	3		6		9		0		2		3		6		3

(c) Finally, add up all of the digits in the second row to get the "Value" of the card:

$$Value =$$

(d) Check if the last digit of the $Value$ is 0. If not, this is definitely not the number of a real card issued by the *Circle Credit Company*. If the last digit is 0, then, most likely, you have a real number of a *Circle Credit* card.

2. Why do you think the company decided to compute the *Value* like this? Why might it be a good idea to use numbers that are next to each other differently when computing the value?

3. Do you think it easy to come up with these credit card numbers? Why or why not? Can you start with an arbitrary 16 digit number and then change some of its digits so that the *Value* ends in 0?

4. *Circle Company Bank* uses the same steps to determine if a bank account number is valid. If the *Value* is divisible by 5 (ends in a 0 or 5), then it is a valid bank account number.
Find the *Value* of the card below:

$$5464\ 3749\ 2372\ 4676$$

5	4	6	4	3	7	4	9	2	3	7	2	4	6	7	6

(a) What is the *Value* of the bank account number?

(b) Could this be a valid *Circle Company Bank* number (Does it end with the digit 0 or 5)?

5. Aside from having a *Value* end in a certain digit, can you think of some other ways that a credit card company or bank might make their card numbers more verifiable?