Your Name:_____

Montlake Math Challenge

February 5, 2009

Introduction: This week's worksheet is all about cryptography. Cryptography is the study of hiding a message in a code so that you can read it and your friend can read it, but a random stranger will not be able to read your message. There are many different types of codes (called **ciphers)** that you can use to **encrypt** a message (put the message into a code) and that your friend can use to **decrypt** the message (translate the code back to your original message). A few of these codes are discussed below.

1. Shift Ciphers

In a shift cipher, we will replace each letter of a message with a different letter in a very specific way. To use a shift cipher, we start by picking a number *n* and we substitute each letter of a message with the letter that occurs *n* letters later in the alphabet As an example, let's pick 3 as our number. Start by writing the alphabet in a row:

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

Since we have chosen our number *n*=3, we will replace each letter with the letter that occurs 3 letters later in the alphabet. We write the new letters below the letters we just wrote:

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
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

Now, to **encrypt** a message, we replace each of its letters with the letter that shows up below it in the above table. For example, if Alice wants to send the message "MATH IS FUN" to Bob, she would encrypt the message "MATH IS FUN," we get

M A T H I S F U N
P D W K L V I X Q

Alice can safely send this message to Bob without worrying about anyone reading it. But how will Bob read it?! Bob needs to **decrypt** the message now. Bob knows that Alice replaced each letter in her original message with the letter that occurs three letters later in the alphabet, so in order to undo this process, he needs to replace each letter in Alice's message with the letter that occurs three letters *earlier* in the alphabet. If he writes the same table as Alice did up above, he converts Alice's message

P D W K L V I X Q

_ _ _ _ _ _ _ _ _

by replacing each letter with the letter that he sees *above* it in the table. For example, the first letter he sees is a P, and the letter he sees above a P in the table is M. Check for yourself that if he decrypts the entire message, he will read Alice's original message.

Exercise 1.1: Encode the following message using the shift cipher on the previous page:

I C A N ' T W A I T F O R V A C A T I O N

_ _ _ _ ' _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Exercise 1.2: Your friend sent you this message using the shift cipher on the previous page. What does it say?

V Q R Z E D O O I L J K W!
_ _ _ _ _ _ _ _ _ _ _ _ _!

Exercise 1.3 Now it's your turn to make up your own shift cipher.

Start by picking your favorite number: _____

Below each letter in the following table, write the letter that occurs your favorite number of letters later in the alphabet. This is the table that you will use to encrypt and decrypt your message:

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

_ _

Now you need to pick a message to encrypt. Encrypt the message "My favorite animal is a _____" (fill in the blank with your favorite animal. What message do you get?

Now exchange papers with a friend. Decode the message you got from your friend to find out his or her favorite animal. Make sure you tell your friend what number you used to encrypt your message!

2. Substitution Ciphers

A substitution cipher is very similar to a shift cipher, except there isn't such a nice pattern that determines the encryption process. As with the shift cipher, we start by writing the alphabet in a row, but now we randomly decide which letters to substitute. The only rule is that each letter can only be used once. For example, we can use the following table:

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

Now, as with the previous example, we **encrypt** a message by substituting each letter in our message with the letter that occurs below it in the following table. For example, to encrypt the message "IT IS RAINING", we would substitute I with the letter that we see below it in the table, which is O. We substitute T with the letter we see below it in the table, which is Z.

Exercise 2.1: Finish encrypting the following message:

```
I T   I S   R A I N I N G
O Z   _ _   _ _ _ _ _ _ _
```

On the other hand, if you receive an encrypted message, you can decode using the same technique as in the previous example. Given an encoded message, you can decode each letter by finding it in the bottom line of the above table and replacing it with the letter you see directly above it.

Exercise 2.2: Someone sends you the following message. If you know they used the above table to encrypt the message, decode it to figure out what it says. A few letters have been filled in for you.

```
S T Z ' L   U G   I X L A O T L!
_ _ T ' _   _ _   _ U _ _ _ _ _!
```

Exercise 2.3: One way to make a substitution cipher is to start with a sentence that is easy to remember. For example, I might use the sentence "The quick brown fox jumps over the lazy dog." I define substitution cipher by substituting A for the first letter of the sentence, B for the second letter of the sentence, and so on, ignoring any letters that I have already used. This is shown in the following table:

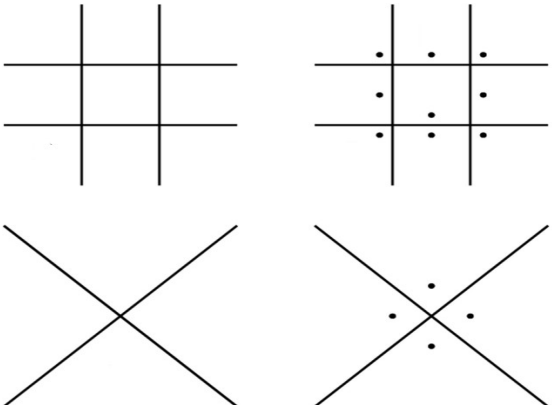
```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
T H E Q U I C K B R O W N F X J M P S V L A Z Y D G
```

Use this table to encrypt the message "_____ is my favorite candy." (Fill in the blank)

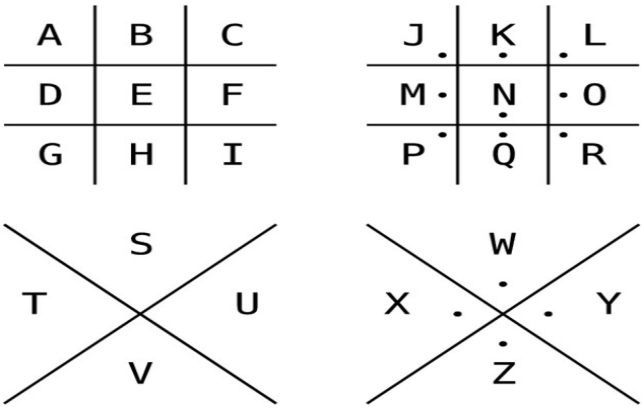
Exchange your paper with a friend. Decode the message you got from your friend to find out his or her favorite candy.

3. Pigpen Ciphers

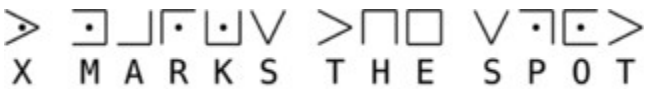
A pigpen cipher is a third type of substitution cipher. In a pigpen cipher, each letter is represented by a symbol instead of another letter. We start with the following grids:



Notice that the grids have 26 spots where we can fill in letters. We might choose to fill them in as follows:



If you want to encode a message to send to your friend, you read each letter out of the grid and draw the shape of the lines and dots that surround it in the grid. This is best illustrated by an example. The message "X MARKS THE SPOT" is encoded as follows:



Exercise 3.1: It's your turn to use the pigpen cipher. Use the pigpen cipher on the previous page to encode the message "I want to take a trip to _____" (fill in the blank).

Now trade papers with a friend and decipher his/her message.

4. **Two-Square Cipher**:

A final cipher is the two-square cipher. It is similar to the substitution ciphers we have seen, but it is a bit more complicated. To use it, we make two 5 x 5 tables. We will put each letter of the alphabet (except J) once in each table. (If you need to encrypt a word that has the letter J in it, you encrypt the J as the letter I and hope the person who is decrypting your message can figure out what you mean.) We might use the following tables:

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

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

Now suppose we want to encrypt the message "Help me, Obi Wan Kenobi." The first step is to break this message up into two letter blocks. We don't worry about spaces between the words here. Instead, we just treat the message as if it were one long block of text that we can break into two letter chunks:

```
HE LP ME OB IW AN KE NO BI
```

Now I will tell you how to encrypt each two letter block of this message. As a running example, we will encrypt the first block, "HE."

Step 1: Locate the first letter of the block in the top square and the second letter of the block in the bottom square. (In bold-face below)

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

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

(continued on the next page)

Step 2: Use these two letters to form a big rectangle that fits over both squares. Look at the new letters in the corners of the rectangle that are underlined below:

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

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

Step 3: Exchange the original letter from the first square (H) with the letter in the opposite corner of the rectangle that also lies in the first square (K).

Step 4: Exchange the original letter from the second square (E) with the letter in the opposite corner of the rectangle that also lies in the second square (W).

Step 5: Repeat this process for each of the two-letter blocks in the original message.

Exercise 4.1: Complete the encoding of the following message. Three of the blocks have been enciphered for you. Notice that in the fourth block OB, the letters O and B lie in the same column of our grid. This means that they form their own rectangle, and nothing changes when we encrypt the block OB. There are extra copies of the squares at the bottom of the page for you to use.

```
HE LP ME OB IW AN KE NO BI

KW QS -- OB -- -- -- -- --
```

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

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

The Two-Square cipher is nice because the decryption process is *exactly* the same as the encryption process. To decrypt a message, we break it up into two letter blocks and follow steps 1-5 above on each of the two letter blocks. There is an example problem on the next page.

Exercise 4.2: Suppose you receive the following message:

BT MR YK IT NZ

Use the following squares to decipher the message. There are extra copies of the squares at the bottom of the page if you need them.

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

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

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

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