NUMB3RS Activity: The Straddling Checkerboard
Episode: "The Janus List"

Topic: Cryptography, number theory, math history **Grade Level:** 9 - 12
Objective: Learn to encrypt and decrypt messages with a straddling checkerboard cipher
Time: 15 minutes

Introduction

In "The Janus List," a bomber gets severely injured when the FBI thwarts his bomb threat. In the hospital, he manages to tap out a sequence of numbers, which Charlie recognizes as a coded message. With some help from Don, Charlie realizes that it is a *straddling checkerboard* cipher, and he is able to uncover the message after experimenting with the cipher. In this activity, students will explore and use the straddling checkerboard cipher.

Discuss with Students

This activity teaches how to use a straddling checkerboard cipher. An encryption method that converts letters and symbols into numbers is called a *cipher*. Any cipher that uses letters in a grid is called a *checkerboard* cipher. This one is called *straddling* because it enciphers some letters as a single number and others as a pair. A person trying to decipher an intercepted message cannot be sure of the locations of the single numbers, so in turn could "straddle" number pairs that should be separate. This would result in a page full of gibberish.

In 1555, Pope Paul IV created the office of Cipher Secretary to the Pontiff. In the late 1580s, this position was held by members of the Argenti family, most notably Giovanni Batista and his nephew, Matteo. Matteo is credited for designing what is now called the straddling checkerboard cipher. This cipher was also used in the 1930s by communist forces during the Spanish Civil War and in later conflicts. Hand-done ciphers like this were mostly used on the battlefield for individual communication between officers. This time period also saw the rise of the Enigma machine for mechanical ciphering, a monumental advance in cryptography.

Student Page Answers:
1. $_{10}C_2 = (10 \times 9) / 2 = 45$ **2a.** *988951587234515* **2b.** *6068697697171202138* **3.** *The first message has 13 characters and uses 15 digits to encipher. The second message has 12 letters and uses 19 digits. The longer message uses fewer digits.* **4.** *Because letters from the keyword are enciphered by a single digit, this would make messages shorter. Also, if there are a lot of frequently used letters in the second or third row, then that row coordinate will appear very frequently in the enciphered message, giving the hint that that digit is a row coordinate.* **5.** *Don't spend a lot of time on this unless you think it is interesting to play with. If you want to give a hint: a common Spanish word (senorita) and people who validate signatures on documents (notaries).* **6.** *bombunderbridge*

L. Charles (Chuck) Biehl, The Charter School of Wilmington, Wilmington, DE

Name: _____ Date: _____

NUMB3RS Activity: The Straddling Checkerboard

In "The Janus List," a bomber gets severely injured when the FBI thwarts his bomb threat. In the hospital, he manages to tap out a sequence of numbers, which Charlie recognizes as a coded message. With some help from Don, Charlie realizes that it is a *straddling checkerboard* cipher, and he is able to uncover the message after experimenting with the cipher. A straddling checkerboard cipher is difficult to break because it enciphers some letters as a single digit and others as a pair of digits. A person trying to decipher an intercepted message cannot be sure of the locations of the single digits, so in turn could "straddle" number pairs that should be separate. This would result in a page full of gibberish.

There are many variations of this cipher. The digits in the first row could be arranged in any order. Commonly, an eight-letter *keyword* (with no repeating letters) is used in the first row of letters (shown below as capital letters). The two numbers not used with the keyword become labels for the last two rows, and can also be anywhere. The remaining cells in these rows are the remaining letters of the alphabet, usually in alphabetical order, with room for a period and a *shift sign*, which is used for enciphering numbers. Here is an example:

	0	9	8	7	6	5	4	3	2	1
	M	A	T	H		C	O	D	E	
1	b	f	g	i	j	k	l	n	p	q
6	r	s	u	v	w	x	y	z	.	/

A cipher is in the form (row, column). The unused numbers in the top row are the only possible row coordinates, so letters from the keyword are enciphered as a single digit.

1. How many different ciphers are possible just by changing where the unused digits go?

To encipher "Janus," the coordinates are (1, 6); (_, 9); (1, 3); (6, 8); and (6, 9). The completed cipher is 169136869. Note that *"a"* has no row coordinate so it appears as a single digit. Whoever receives the message—and has the key, of course—knows that whenever there is a 1 or a 6, it is the beginning of a pair. Word breaks—the spaces between words—are not enciphered. That would provide another clue for an interceptor.

2. Encipher these:
- **a.** "attack the dock" _____
- **b.** "rush shipment" _____

3. Compare the length of each message to the length of its cipher. What do you notice?

4. The most frequently used letters (in descending order) in the English language are **e-t-a-o-i-n-s-r**. Some variations of the straddling checkerboard cipher use these letters instead of a keyword. Why could this be a good idea?

5. One argument for using a keyword instead of the letters above is ease of memorization. One way is the mnemonic "Estonia-R." What two common, and therefore easily memorized, words can be formed from the letters "e-t-a-o-i-n-s-r"?

6. Decipher: 1040106813326010601731 82

L. Charles (Chuck) Biehl, The Charter School of Wilmington, Wilmington, DE

The goal of this activity is to give your students a short and simple snapshot into a very extensive mathematical topic. TI and NCTM encourage you and your students to learn more about this topic using the extensions provided below and through your own independent research.

Extensions

Introduction

The straddling checkerboard cipher is one of many historical ciphers and codes. The terms *cipher* and *code* are often used interchangeably. The main difference is that ciphers substitute or change single letters or letter pairs, while codes substitute entire words, phrases, or sets of numbers. Ciphers and codes have appeared throughout history, dating back to about 4,000 years ago.

For the Student

- To use the cipher in this activity to send numbers, the "/" character is used at the beginning and end of a set of numbers. Often each digit is doubled to decrease transmission errors. For example, the message "I need 500 sandwiches" gets ciphered as INEED/500/SANDWICHES ("61" is the "/") and so the cipher becomes: 171322361550000616991336617572 69.

- For additional security, a straddling checkerboard can be given another layer of encipherment in the form of adding a secret *key number* to the cipher before sending it. Suppose the first five digits of π are chosen as the key number: 31415. This is added to the cipher using non-carrying addition (just record the ones digit), so the previous cipher becomes:

  $$\begin{array}{l} 171322361550000616991336617572 69 \\ +\ 31415314153141531415314153141531 \\ \hline 485475402081415920044477148987 90 \end{array}$$

- For even **more** security, this cipher could be run through the same straddling checkerboard cipher to turn it back into letters producing:
  OTCOHCOMEMTLKAEMMOOOHHLTATHAM

- Using the checkerboard and the key number, recover the original message.

Related Topic

Other examples of historical ciphers include the Caesar (shift) cipher, rail fence (or Freemason's) cipher, the ADFVDX cipher (World War 1), Vigenère ciphers, and an almost endless list of others, all of which are very interesting to study. Probably the most famous of the mechanical ciphers is ENIGMA (World War 2). There are many books and Web resources available to learn about these ciphers and their importance in history.

Additional Resources

For an interactive introduction to the general concept of cryptography, see:
http://williamstallings.com/Crypt-Tut/Crypto%20Tutorial%20-%20JERIC.swf

An excellent book on codes and ciphers throughout history is Simon Singh's *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*.

L. Charles (Chuck) Biehl, The Charter School of Wilmington, Wilmington, DE