NUMB3RS Activity: **Code Crackers**
Episode: "Assassin"

Topic: Simple Codes **Grade Level**: 6-12
Objective: Making and breaking codes
Time: about 15 minutes

Introduction

Codes have been used for centuries as a way to communicate in secret. In order for codes to work, you need code makers (cryptologists) and where there are code makers there are often code breakers (cryptanalysts). There have been many famous codes; some very simple, such as the Caesar substitution cipher (seen below); some very complex, such as RSA encryption which utilizes very large prime numbers and is widely used in electronic commerce. Advanced codes employ the best minds and computer systems in the world.

Discuss with Students

In **"Assassin**,**"** Agent Don Eppes has intercepted a coded message that he brings to his brother, Charlie, for decrypting. Charlie recognizes the code as a *cipher* (a code that substitutes letters for other letters or small groups of letters), and realizes that a computer is not needed to break it. An example of a simple cipher is below.

Introduce making a code with a *key*. In the example below, the key shows what each letter will be replaced with. If you know the key, you can write in the code and read anything written in it. When you replace, or "substitute" a letter, you are using *substitution*.

For example, in this key, the alphabet has been shifted **9** places. Instead of communicating the entire alphabet shift to someone, you could simply give them a number as the key. The key for this code is **9**.

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**
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

- Using the above key, **9**, decode the following message:
  YVCG DV UFE. [*HELP ME DON*]
- What letter appears more than once in the coded message above?
  [*V*] To what uncoded letter does it correspond? [*E*]

Identifying common letters and words can be used to help break codes. "E" is the most commonly used English letter, followed by "A", "O" and "T". With long messages, you can count each coded letter and make educated guesses about what they stand for.

Student Page Answers: **1.** *Meet me tonight at seven place to be named*; **2.** *Getty Center east entrance*. **3**. *25; then it repeats* **4***. Try each of the 25 keys or look for used letters for a clue.* **5***.* **a***. Key of 21;* **b***. Keys of 41, 67, and 93.* **6**. **a**. *answers may vary; possible answer: assign letters randomly instead of in order* **b***. answers will vary; possible answer: the receiver would need the entire alphabet and which letter went with which.*

Name: _____ Date: _____

NUMB3RS Activity: Code Crackers

Agent Don Eppes intercepted two messages that Charlie decided used the substitution codes with keys 6 and 25. Use the charts and the keys to help you decode the messages below.

1. *Message*: GYYN GY NIHCABN UN MYPYH JFUWY NI VY HUGYX *Key:* 6

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

_____

2. *Message*: HFUUZ DFOUFS FBTU FOUSBODF *Key:* 25

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

_____

Answer the following questions about the type of substitution code used above.

3. How many unique keys are there? Explain why there aren't more.

_____
_____

4. If someone intercepted a coded message and wanted to read it without the key, what could they do to break it? _____
_____

5. Shifting the alphabet 1 space is the same as shifting the alphabet 27 spaces.

a. If Charlie found someone using a key of 47, what might that mean?

_____

b. Find three other keys that are equivalent to a key of 15.

_____

6. **a**. How could you make a substitution code that is harder to break?

_____

b. What key would the receiver need in order to read the message?

_____

Extensions

Activity: Two More Hand Codes

Pig Pen Cipher: In the pig pen cipher, pens are formed for letters by the spaces in a tic-tac-toe grid as shown.

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

Letters are coded by their placement in the "pens" in which they are found. Letters A-I are coded by sides of the their pens and with no dots, letters in the second grid shown with pens having one dot and letters in the third grid shown in pens with as two dots. Some examples are shown below:

A = **F** = **L** = **N** = **V** = **Y** =

Example:

Rail Fence Cipher: To encode a message, write it in a table with columns of a given length. Consider the message "Come alone we have your brother" written in the table below. Note that the trailing letters G and A are used to complete the grid – without them, you would not be able to decipher the code.

1	**C**	**A**	**E**	**A**	**O**	**R**	**E**
2	**O**	**L**	**W**	**V**	**U**	**O**	**R**
3	**M**	**O**	**E**	**E**	**R**	**T**	**G**
4	**E**	**N**	**H**	**Y**	**B**	**H**	**A**

Then write the text out reading from left to right:

CAEAOREOLWVUORMOEERTGENHYBHA

This string of jumbled letters is your coded message. The length of the column (a number) is the key. The key for this code is **4**.

To decode it this message, use the key, **4**, and separate the text into **4** groups of equal length:

C A E A O R E **O** L W V U O R **M** O E E R T G **E** N H Y B H A

Now reading the 1st letter of each group, then the 2nd letter of each group, and so on, will reveal the coded message.

Example: T G N M G H L D I H E E S D T E L A N R A A T I E *Key*: 5

For the Student

- Use each of the hand codes above to code your own messages.
- Often, more than one cipher is applied to the same message. Combine hand codes to make your code even more difficult to decipher.

Research the history of cryptography and the use of different codes.

- In the 1500s, Mary Queen of Scots used a code to plot an assassination. Learn about the code she used and the outcome of her scheming.
- During World War II, Germany used a machine to encode its messages. Learn about the enigma machine and how it worked.
- Also during World War II, American troops used Navajo “code talkers” to communicate in the field. Learn about this unique form of “encrypted” communication. Why was the Navajo language so useful in this situation?
- Edgar Allen Poe had an interest in cryptography, and even cracked codes submitted by readers of a newspaper. Learn about Poe’s code-cracking abilities and the challenge he posed that took over 100 years to solve.
- For advanced students: the RSA cipher uses a key that can be made public. Learn how very large prime numbers are used to encrypt messages in this cipher.

Resources:

http://www.simonsingh.net/The_Black_Chamber/contents.htm
Simon Singh has written a very readable book entitled *The Code Book: How to Make It, Break It, Hack It, Crack It*. This companion website has many pages on the history and uses of cryptography.

http://illuminations.nctm.org/tools/tool_detail.aspx?id=5
This interactive math applet from Illuminations can be used to explore math and create interactive lessons. This applet allows you to explore a substitution cipher by encoding and decoding text messages. Shift transformation and the stretch value are introduced.

