NUMB3RS Activity: Onion Peeler
Episode: “Killer Chat”

Topic: Computer Science **Grade Level:** 10 - 12
Objective: Follow a message through an Onion Routing Network.
Time: 20 - 30 minutes

Introduction

In the episode “Killer Chat,” the killer streams videos of confessions over the Internet. To help trace the origins of the streaming video, Charlie discovers that the killer is hiding his online location through an onion routing scheme. Charlie explains that such a scheme is a way of sending content over a network while staying anonymous.

Discuss with Students

One of the first things students must do is use the algorithm to convert from the Hexadecimal Router Number to the Decimal Router Key. Changing from hexadecimal to decimal numbers is something students may not have experience with, so you may wish to either convert them as a class or spend a few minutes explaining how they can convert them.

Use the table below to help illustrate the concept of the base-16 Hexadecimal numbers.

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Dec	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Hex	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Dec	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

The students should notice that the digits 0–9 are the same for both number systems and that the letters A–F are used to represent the decimal values 10–15. To convert between them, multiply each digit by a power of 16, where the power is dependent on the place value. We notice from the table above Hex-1C would be (1 • 16) + 12or Dec-28. For our three digit hexadecimal router number, we can generalize the three digits so *XYZ* would convert to $\left(X \bullet 16^2\right)+\left(Y \bullet 16^1\right)+\left(Z \bullet 16^0\right)=$ Decimal Number.

Note that the only parts of the router number used in determining the next router are the first and the last digits; the middle digit could be kept secret. By publishing the first and last digits and keeping the second digit secret, this introduces the notion of public key encryption. It also leads students to the interesting question of how many routers could our system contain. Because there are 15 choices for the first digit and 15 choices for the last digit, students might think that there would be 225 possibilities. However since we are limited to a three-digit Router Key, then Dec-999 is Hex-3E7, so we actually have 3 choices for the first digit and 16 choices for the last, which gives a total of 48.

Brock Wenciker, Shawnee Mission East High School, Overland Park, KS

Student Page Answers:

Path of message: 1C3→26B→3AD→2F4→36C

Router Number	Router Key	(Even)						Message				(Odd)					
1C3	451	**A**	D	2	3	**2**	3	D	4	W	3	C	A	R	4	E	B
26B	619		**D**	2	3	A	3	D	4	W	**3**	C	A	R	4	E	
3AE	942			2	3	A	3	D	4	W	D	**C**	A	**R**	4		
2F4	756				3	A	3	D	**4**	**W**	D	R	A	C			
36C	876					A	3	D	W	4	**D**	**R**	A				
Message							3	D	W	4	R	D					

1. *3DW4RD is Edward.* **2.** *2CA*

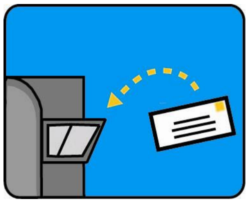
Brock Wenciker, Shawnee Mission East High School, Overland Park, KS

Name: ___________________________________ Date: ________________

NUMB3RS Activity: Onion Peeler

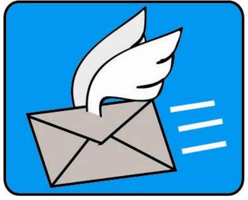
In the episode “Killer Chat,” the killer streams videos of confessions over the Internet. To help trace the origins of the streaming video, Charlie discovers that the killer is hiding his online location through an onion routing scheme. Charlie explains that such a scheme is a way of sending content over a network while staying anonymous.

Think of it like mailing a series of envelopes inside envelopes.

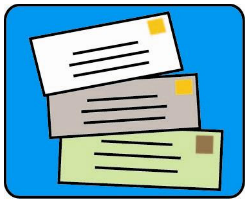


An envelope is mailed to the name on the address.

Inside the envelope is another envelope which is mailed to the second address.



Inside the second envelope is yet another envelope. Again this is forwarded to the next address.



This continues until finally the message is revealed inside the last envelope: “Buy more envelopes.”

In the end, the person who is told to buy more envelopes does not know where or by whom the original envelope was mailed. Each envelope is like a layer of an onion that is peeled back until the message inside reaches the end. It works the same on the Internet, except instead of envelopes, the sender uses a series of routers, and instead of opening envelopes, the routers use a decryption algorithm.

The following is a decryption algorithm used to trace a message through the onion routing network. A sample message is used.

<table>
<tr><th>Steps</th><th>Example</th></tr>
<tr><td>Each router has been assigned a three-digit hexadecimal number. Hexadecimal (base-16) numbers are used in computer languages, such as HTML. They are written with the digits 0–9 and the letters A–F. For our onion routing network, translate the hexadecimal routing number into a three-digit decimal number. This decimal number is the Router Key.</td><td>Router 1AD would translate to
$\left(1 \cdot 16^{2}\right)+\left(10 \cdot 16^{1}\right)+(13 \cdot 16^{0})=429$<table><tr><td>4</td><td>2</td><td>9</td></tr><tr><td>The first digit is even, so start counting from the left</td><td colspan="2">Switch the second and the ninth characters in the code</td></tr></table></td></tr>
<tr><td>The first digit indicates the direction to start counting from (even is from the left, and odd is from the right), and the second and third digits indicate the positions of the two characters that must be switched.</td><td>Count from the left and switch the second and ninth characters:
2<b>A</b>4BY3NR<b>5</b> → 2<b>5</b>4BY3NR<b>A</b></td></tr>
</table>

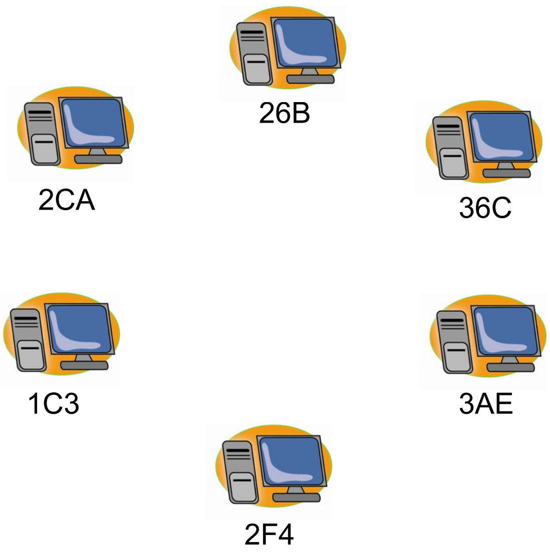
Brock Wenciker, Shawnee Mission East High School, Overland Park, KS

Remove the first and the last characters from the message. These are the first and the last digits of the next router.	Removing 2 and A, the remaining message 54BY3NR would be sent to a router such as 2CA.
Repeat the decryption algorithm until the first and last characters are AA. This is the end code.	

For this activity, Charlie's middle name has been encrypted. As you decode his middle name below, trace the path of the message as it passes through the onion routing network.

Convert the Router Numbers from their Hexadecimal Router Number to their corresponding Decimal Router Keys.

Router Number	Router Key



Router Number	Router Key	(Even)							Message								(Odd)
1C3		A	D	2	3	2	3	D	4	W	3	C	A	R	4	E	B
Message																	

The message may still seem encoded but actually it is written in 1337 (Leet) speak. In the episode, Charlie and the FBI analyze online chat from the killer and find much of it is written in Leet speak. Leet speak is a modification of written text where numbers and symbols are often used to replace letters. For example, the show's title *NUMB3RS* uses the number 3 in the place of the letter "E."

1. What is Charlie's middle name?

2. Which router was not used in the onion routing scheme?

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

To encode a message, we must reverse the algorithm. For example, to encode the word **Calculus** we can first translate it into Leet speak.

<table>
<tr><th>Steps</th><th>Example</th></tr>
<tr><td>First, translate the message into Leet speak.</td><td>Calculus ↦ K4LCULUZ</td></tr>
<tr><td>Add the letter A to the beginning and end of your message.</td><td>AK4LCULUZA</td></tr>
<tr><td>Using the Router Key that corresponds to a particular Router Number that you choose, switch the specified characters. The first digit indicates the direction to start counting from (even is from the left, and odd is from the right), and the second and third digits indicate the positions of the two characters that must be switched.</td><td>The Router Key for Router 2F4 is 756.
<table>
<tr><td>7</td><td>5</td><td>6</td></tr>
<tr><td>The digit is Odd, so start counting from the right</td><td colspan="2">Switch the fifth and sixth characters in the code</td></tr>
</table>
AK4LCULUZAA ↦ AK4**CL**ULUZAA</td></tr>
<tr><td>Add the first and third letters of the router you wish to use next to the beginning and end of your message.</td><td>For the router 2F4, add 2 to the beginning and 4 to the end of your message.
2AK4CLULUZAA4</td></tr>
<tr><td>Repeat these steps several times choosing different routers until the message is encrypted.</td><td>1C3 **C**AK4**2**LULUZAA4
1CAK42LULUZAA43
26B **L**CAK42LU**1**UZAA43
2LCAK42LU1UZAA43B
3AE 2LCAK42LU1UZA**3**4**A**B
32LCAK42LU1UZA34ABE
36C 32LCA**4K**2LU1UZA34ABE
332LCA4K2LU1UZA34ABEC
26B **2**32LCA4K**3**LU1UZA34ABEC
2232LCA4K3LU1UZA34ABECB
2F4 2232LCA4K3LU1UZA3**A4**BECB
22232LCA4K3LU1UZA3A4BECB4</td></tr>
<tr><td>Encoded Message</td><td>22232LCA4K3LU1UZA3A4BECB4</td></tr>
</table>

Using the encoding algorithm and router numbers from the activity, encode a message, and then have a classmate decode it.

Additional Resources

The applet at this Web site converts numbers between decimal, binary, and hexadecimal forms: **http://www.willamette.edu/~gorr/classes/cs130/lectures/BinaryConversion/convert.html**

The onion routing network, or Tor, has hundreds of thousands of users. Read how Tor works at the site: **http://tor.eff.org/overview.html.en**

Fort Consult wrote a paper on Practical Onion Hacking published in October 2006. You can read the report at **http://www.packetstormsecurity.org/0610-advisories/Practical_Onion_Hacking.pdf**.