JULY 2014 VOLUME 1 ISSUE 1

CLANDESTINE AFFAIRS

THE NEWSLETTER FOR ALL THINGS RELATED TO CRYPTOGRAPHY

The Kryptos sculpture outside CIA headquarters in Langley, Virginia has challenged many to try to decrypt what is written on it.

LEARN MORE ABOUT CRYPTOGRAPHY FROM THE WEBSITES BELOW!

1. **The Cryptoclub Project (www.cryptoclub.org)**
   Try out your code cracking skills with challenges and games. Cipher tools are provided.
2. **Journey into Cryptography (www.khanacademy.org/math/applied-math/cryptography)**
   This site provides text, pictures, and videos to explain a variety of codes and ciphers.
3. **Crypto-challenge (www.khanacademy.org/math/applied-math/applied_math_challenges/cryptochallenge/a/introduction)**
   Solve the ciphers in this challenge to test your code and cipher skills.
4. **Cryptokids (www.nsa.gov/kids/)**
   Visit this site (part of the NSA) for games, activities, and additional links to code breaking sites!
5. **Math Illuminations Codes (http://illuminations.nctm.org/Activity.aspx?id=3543)**
   With this activity, explore creating a cipher that uses a Caesar shift with a twist.
6. **Cipher Tools (http://runkin.com/tools/cipher/)**
   Visit this site to use many tools to encipher and decipher messages! Our frequency tool is on this website.

To Our Parents…
An Introduction to Our Cryptography Session

Cryptography, the practice of secret communication, has been an interest of people for millennia--from ancient military and political uses to modern uses that enable us to communicate and shop online safely and securely! Perhaps you even used some codes or ciphers as a child! Igpay Atinlay, anyoneway? (Pig Latin, anyone?)

This week, your child will be challenged to create a new code or cipher that will be secure enough to help a team of fifth graders at D.F. Walker Elementary School in Edenton, North Carolina securely communicate with each other as they participate in a competition. In order to help your child do this, we will provide your child with the opportunity to learn a sampling of established code systems, monoalphabetic ciphers, polyalphabetic ciphers, and transposition ciphers. They will also learn a couple of cipher breaking techniques that revolutionized the world of cryptography! Using all these established resources, the students will determine how they can improve on the codes and ciphers of the past to create the best one to help our "client" team of students!

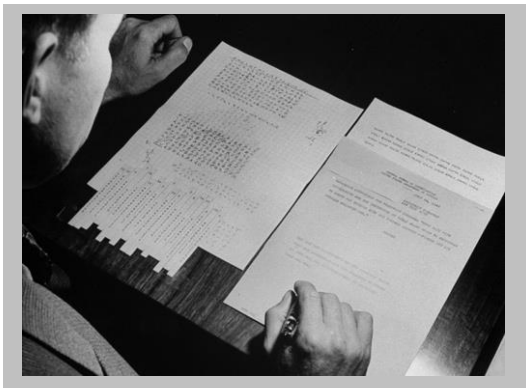
We hope the students will be so excited at the end of the week (or even during the week) that they will want to learn more! We have ideas for further learning in this newsletter and resources the students can use are listed and linked on our website (cryptography2014.weebly.com). We know this will be a great week of learning!

For more information, check out these kid- and adult-friendly books:
The Cryptoclub: Using Mathematics to Make and Break Secret Codes by Janet Beissinger and Vera Pless
Mysterious Messages: A History of Codes and Ciphers by Gary Blackwood
Top Secret: A Handbook of Codes, Ciphers, and Secret Writing by Paul B. Janeczko

SHHH….IT'S A SECRET: LEARNING THE KEY TO CRYPTOGRAPHY

Nancy Heiniger and Carol Tuttle
ECU/Pitt County AIG Camp
July 7-10, 2014
cryptography2014.weebly.com

Inside this Issue



Picture of a person working to crack the Enigma cipher

POINT TO PONDER:
WHEN CREATING A CRYPTOSYSTEM, THE TIME NEEDED TO DECIPHER A MESSAGE SHOULD BE CONSIDERED AS IMPORTANT AS THE ALGORITHM USED.

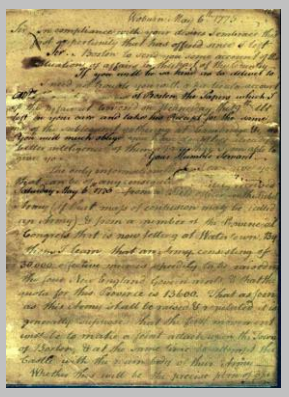
There are many factors that cryptographers need to consider when creating a cryptosystem. It would be great to create a totally secure cryptosystem, but how long would it take the receiver of such an encrypted message to decrypt it? According to legend, as an ancient Celtic hero, Bres, was about to go into battle, he received a secret message using an unusual cipher. He got so caught up in trying to decipher it that he lost the battle! Later in history, during the United States Civil War, a confederate officer was so confused trying to decipher a Vigenère cipher that, after trying to decipher it for twelve hours, he finally rode his horse around enemy lines to talk with the sender in person! Stories like these continue through history and demonstrate that, while creating the most secure cipher possible with a complex and challenging algorithm that would bewilder an adversary is important, if the message takes too long to decipher, the cipher is still ineffective!

CRYPTOGRAPHY: MORE THAN JUST CODES AND CIPHERS!

Although we are only discussing codes and ciphers during our sessions this week, cryptography also has other techniques for hiding messages. One of these techniques is steganography—concealing a secret message. Ancient methods of steganography included carving a message into a plank of wood and then covering the message with wax. A casual observer of the wood would not even realize there was a message. However, when the wax was melted, the message was revealed. Other ancient methods included hiding messages in bandages put on soldiers on the battlefield or sewing a message onto the sole of a sandal. Confederate soldiers even used microphotography to hide small pictures of orders inside their buttons. These messages were not perceptible to the naked eye but could be viewed using a strong magnifying lens!

Some interesting (and fun) methods of steganography include the following:

- **Hide a message within a longer message (null cipher)**
  The receiver of the message would know to only use certain letters in the longer message to make the true message. For example, they would look at the first letter of each word, the last letter of each word, every fifth letter, etc. The rest of the letters in the message are simply used to conceal the true meaning.
- **Hide a message using invisible ink**
  The sender of a message writes the message using a substance that is invisible once it dries. The receiver of the message "develops" the substance (perhaps using heat or another substance) so that the message becomes visible.
- **Hide a message in a newspaper or other printed page**
  The sender of this message uses a pin to create tiny holes in the paper under the letters that are needed for the message. These pin holes are too small for people to notice, but when the receiver holds the paper up to the light, the holes and the message are evident.



An invisible ink letter treated with a chemical reagent from British spy Benjamin Thompson, 1775 (From the collection of the Clements Library)

MODERN CRYPTOGRAPHY ADDRESSES WAYS TO DETERMINE THE RELIABILITY OF INFORMATION SENT ONLINE. IT PROVIDES WAYS TO VERIFY THAT THE INFORMATION SENT HAS NOT BEEN CHANGED IN ANY WAY!

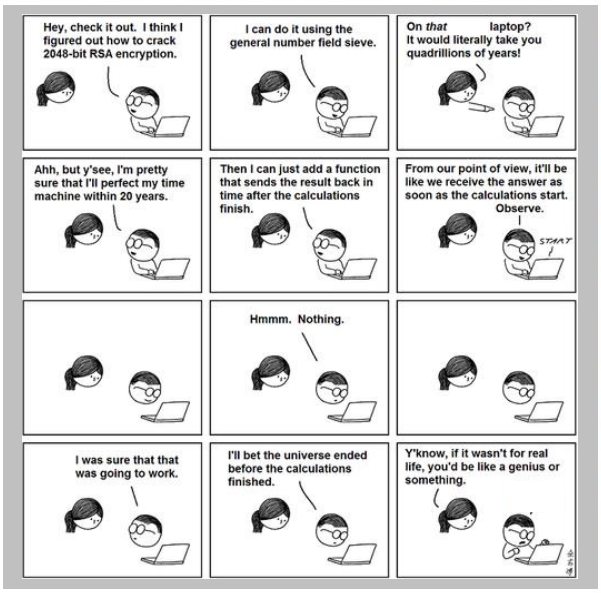
"Securing a computer system has traditionally been a battle of wits—the penetrator tries to find the holes and the designer tries to close them."
--Gosser

POINT TO PONDER:
SECRETS ARE NECESSARY FOR A STABLE SOCIETY.

According to CNN (May 2014), identity theft is on the rise and hits a new American every two seconds. If you've ever been the victim of having your passcodes or credit card information hacked and stolen, then you know what kind of chaos that can cause. The amount of time it takes to recoup financial losses and to get back to "normal" can take weeks if not months. This is a very personal reason why secrets are necessary for a stable society. If our personal information were not encrypted, then anyone could hack into our banking accounts and the result would be mass pandemonium.

Military secrets, on the other hand, don't seem to make as much of an impact on us personally. However, if we didn't have those secrets, our very own democracy could be affected. The unauthorized release of military secrets can compromise our nation's national security and can cause harm to come to our military and civilian personnel serving in war zones.

The December 2013 Target security breach was the largest in U.S. history.



Cartoon demonstrating the time needed to crack a cipher

POINT TO PONDER:

CRYPTOSYSTEMS DO NOT HAVE TO BE ABSOLUTELY SECURE.

There is only one theoretically totally secure cipher, the one-time pad. Using that system, each key must be as long as or longer than the text that is being enciphered. Also, each key can only be used once or an adversary might gain enough clues to crack the cipher. Obviously, this would pose some practical problems! Therefore, cryptographers have turned their attention to cryptosystems that are "secure enough." These systems can be cracked, but the time it would take to crack the cipher is so great that, by the time the information could be intercepted and decrypted, it would be outdated! Even the system used to make internet communication and commerce between people who do not know each other possible, RSA, uses a known algorithm. All it takes to break the cipher is determining the very large prime factors of very large numbers! Fortunately, this is extremely time consuming—even for networks of computers!

MODERN CRYPTOGRAPHY ADDRESSES WAYS TO VERIFY THAT THE PERSON YOU BELIEVE SENT INFORMATION TO YOU ONLINE ACTUALLY DID THE SENDING; IT PROVIDES WAYS TO AUTHENTICATE THE SENDER OF INFORMATION!

There are two types of cryptography: One that will keep your kid sister from reading your information and one that will keep computers from reading your information.

JULY 2014 VOLUME 1 ISSUE 1

Model of the Spartan scytale—a device for creating a transposition cipher

A replica of the type of cipher wheel Thomas Jefferson used

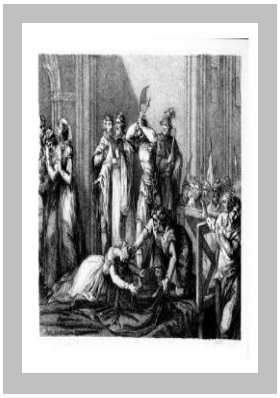
IDEAS FOR EXTENSION: CHANCES TO LEARN AND CREATE MORE!

Use the resources on our website (cryptography2014.weebly.com/activities) to help with the following activities.

1. **Create a scytale—an ancient cipher tool.**
2. **Create a version of Thomas Jefferson's Cipher Wheel.**
3. **Create and conduct a survey of people you know to see if they realize how often cryptography is used in their everyday lives (ex. banking, cell phones, passwords, etc.).**
4. **Create a way to inform people about the ways cryptography is used in everyday life (newsletter, podcast, flyers, etc.).**
5. **Make a "cryptography kit" that includes tools we have learned about this week, any tool(s) needed for your cryptosystem, and other tools found on this list or on the resources on our website.**
6. **Research the German Enigma Machine and the difference it made in World War II.**

Point to Ponder:
A Code is Only as Good as its Key.

In Elizabethan England, Mary, Queen of Scots sent coded messages to her supporters who were plotting to murder Queen Elizabeth. The messages were intercepted and deciphered by the head of Elizabeth's secret service, which resulted in Mary's execution. Codes that are too simple do not provide the degree of secrecy needed to complete their purpose. On the other hand, a code that is too difficult to decode can have the same outcome. It is vital that the key to breaking the code be complex enough that only the person who has the key can break it!



The execution of Mary, Queen of Scots

EXPERIMENT WITH THESE ACTIVITIES

What is the Best Invisible Ink?

1. Research to find different substances that could be used to make invisible ink. Possible resources for research are located on our website (cryptography2014.weebly.com/activities).
2. Choose at least 5 of the substances to test (with your parents' permission).
3. Determine the criteria that you will use to decide which substance is the best. [Which one is easiest to use? Which one disappears most completely when dry? Which one shows up the clearest when it is developed (when the information is revealed)? And so on…]
4. Test the substances you chose in step #2.
5. Report your findings to your friends. Maybe you can use the best substance(s) to share secret information with one another.
6. To learn even more, research to find out why these substances work as invisible ink.

Which is the most secure spoken code?

1. Research and become fluent using at least 3 spoken codes. Possible resources for research are located on our website (cryptography2014.weebly.com/activities).
2. Find participants for your experiment. These participants should not already know the codes you will be using.
3. Have each participant listen to you say a common phrase using the first spoken code. Repeat the phrase (in code) as many times as necessary. Record the number of repetitions needed for the participant to understand what you are saying.
4. Repeat step 3 with each of the spoken codes you are testing.
5. Repeat your test with at least 5 people.
6. Determine which of the codes required the most repetitions to be understood by someone who did not know the key to the code.

MODERN CRYPTOGRAPHY ADDRESSES ENCRYPTION SYSTEMS THAT ALLOW PEOPLE WHO DO NOT KNOW EACH OTHER TO INTERACT WITH ONE ANOTHER SECURELY AND CONFIDENTLY; THIS MAKES INTERNET COMMUNICATION AND COMMERCE EFFECTIVE!

"Human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

Edgar Allen Poe