Cryptography – March 16, 2015

CRYPTOGRAPHY – (8 points)

What is *Cryptography*?

Cryptography has been used for thousands of years to protect secret information. You may have learned how the United States and its allies used cryptography during World War I and World War II, but with the use of computer systems and the internet, cryptography has become more important, especially in the computer science field of security (http://en.wikipedia.org/wiki/History_of_cryptography).

According to http://www.webopedia.com/, Cryptography is:

> "The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable."

Cryptography is used to help protect email, credit cards, and many different types of data. Computer Scientists need to use cryptography when developing security systems.

To learn more, we recommend watching the Khan Academy video, "What is Cryptography."

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography

Let's get started!

Choose one option that best fits your student's level of experience.

Option A - ***The Pigpen Cipher*** (Beginner/Intermediate)*

The Pigpen Cipher uses symbols to represent letters of the alphabet and has been used by many groups for many years. The cipher was used by the Freemasons, a secret society in the 18th century, and by Union troops during the Civil War. See if you can decode the message and create your own.

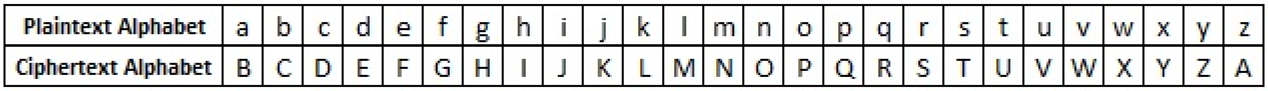
1. Open the *Pigpen Cipher* worksheet. Go to http://ou.montana.edu/csoutreach/Looney-challenges/PigpenCipher.pdf to open the worksheet.
2. Decipher the words using the diagram. What are the two words?
3. Answer the questions – you may answer the questions individually or with a friend/partner.

Option B – **Breaking the Code** (Intermediate/Advanced)*

1. Open the *Breaking the Code* worksheet. Go to http://ou.montana.edu/csoutreach/Looney-challenges/crypto-maths.com_breaking_the_code.pdf to open the worksheet.
2. Decipher the message using a Mono-alphabetic Substitution Cipher. A "monoalphabetic substitution cipher, also known as a simple substitution cipher, relies on a fixed replacement structure. That is, the substitution is fixed for each letter of the alphabet. Thus, if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext. A simple example is where each letter is encrypted as the next letter in the alphabet: "a simple message" becomes "B TJNQMF NFTTBHF". In general, when performing a simple substitution manually, it is easiest to generate the

* Adapted from Crypto.interactive-maths.com

ciphertext alphabet first, and encrypt by comparing this to the plaintext alphabet. The table below shows how one might choose to, and we will, lay them out for this example.



Plaintext Alphabet	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
Ciphertext Alphabet	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	A

There are many different monoalphabetic substitution ciphers, in fact infinitely many, as each letter can be encrypted to any symbol, not just another letter (http://crypto.interactive-maths.com/monoalphabetic-substitution-ciphers.html).

3. Use the Grids page to help you record letter to break the code. You may want to print the worksheet and the grid.
4. Some helpful hints:
   - What is the most common letter in English? (E)
   - What words in English only have 1 letter? (A or I)
   - What 3 letter words in English are most common (e.g. ‘And’ and ‘The’)
5. After completing the message, answer the two questions at the bottom of the page.

How to earn points:

1) If you haven’t registered your class, please go to cs.montana.edu/looney-challenge and click on the “Register for Looney Challenges” link.
2) Discuss with your class the difficulty of the activity. What did they learn? How difficult was the activity? Do they understand the concept?
3) Briefly, in a couple of sentences, describe in your email what happened during the activity? Did your students understand the concept(s)? Email your description to looneychallenges@gmail.com
4) If you want to attach an example, photographs of students working, or video of student’s outcomes, please send them as an attachment.
5) We will send you a confirmation and provide you your point total for the activity and your total points for Looney Challenges.

All Looney Challenges can be completed at any time during the 2015-2016 school year. All Challenges are due, June 30, 2016.

Questions? Please send an email to looneychallenges@gmail.com or call Sharlyn Izurieta at (406) 994-4794.

DEADLINE is June 30th, 2015.

* Adapted from Crypto.interactive-maths.com