Cryptography Using Linear Functions and Their Inverses

NCTM Annual Meeting and Exposition 2015

Kara Leaman

kara.leaman11@gmail.com

Ann Schlemper

aschlemper@ccis.edu

CRYPTOGRAPHY PROJECT

REQUIREMENTS for PROJECT WITH PARTNER:

1. Each cryptogram is displayed along with the solution.
2. The process of coding is explained.
3. The process of decoding is explained.
4. Describe how arithmetic works inside the system mod 26.
5. Explain how the use of *inverse functions* made the coding and decoding possible.

REQUIRED INDIVIDUAL WRITTEN WORK TURNED IN THROUGH GOOGLE CLASSROOM:

6. Research at least one of the following and summarize in at least 200 words:
    a. Find at least two careers which make use of cryptography.
    b. What is the type of cryptography we used in this project? Provide some history or usage for this type of cryptography.
    c. What type of math would I study to learn more about mod arithmetic?
    d. Provide some historical foundation for cryptography, including a specific event if you desire.
    e. Describe a circumstance in which cryptography is used currently.
    f. How are cryptograms made which appear in the newspaper?
7. Reflection paragraph (included separately for each person)
    a. How did you divide the workload with your partner? Did each person contribute equally?
    b. What did you like/dislike about this project?

CHOICE OF PRODUCT:

1. Prezi (www.prezi.com) – if using this be sure to share a link to your project with me – leamank@unity.k12.il.us
2. Powerpoint or Google Slides
3. Video – you are welcome to use my iPad to do this, but may need to schedule a time before or after school with your partner
4. Booklet – be creative! Write a story!
5. Poster – ability to read from 6 ft away

BONUS POINTS WILL BE GIVEN FOR MORE CREATIVE PROJECTS!

GRADING: 50 points – READ the rubric!

CATEGORY	5	4	3	2 OR 1
Content X 3	Covers topic in-depth with details and examples. Subject knowledge is excellent. (x3)	Includes essential knowledge about the topic. Subject knowledge appears to be good. (x3)	Includes essential information about the topic but there are 1-2 factual errors. (x3)	Content is minimal OR there are several factual errors. (x3)
Requirements X 2	All requirements are met and exceeded. (x2)	All requirements are met. (x2)	One requirement was not completely met. (x2)	More than one requirement was not completely met. (x2)
Attractiveness	Makes excellent use of font, color, graphics, effects, etc. to enhance the presentation.	Makes good use of font, color, graphics, effects, etc. to enhance to presentation.	Makes use of font, color, graphics, effects, etc. but occasionally these detract from the presentation content.	Use of font, color, graphics, effects etc. but these often distract from the presentaion content.
Organization	Content is well organized using headings or bulleted lists to group related material.	Uses headings or bulleted lists to organize, but the overall organization of topics appears flawed.	Content is logically organized for the most part.	There was no clear or logical organizational structure, just lots of facts.
Originality	Product shows a large amount of original thought. Ideas are creative and inventive. (+5)	Product shows some original thought.	Uses other people's ideas (giving them credit), but there IS little evidence of original thinking.	Uses other people's ideas, but does not give them credit.
Perseverance	Product shows a large amount of trial and error in decoding or is longer than most. Logic behind guesses is explained.	Product shows a some amount of trial and error in decoding. Logic behind guesses is explained.	Product shows some amount trial and error in decoding. Logic behind guesses is not explained.	Product does not show any trial and error in decoding. Logic behind guesses is not explained.
Workload	The workload is divided and shared equally by partners. (Evident in reflection)	The workload is divided and shared fairly by partners, though workloads may vary from person to person. (Evident in reflection)	The workload was divided, but one person in the group is viewed as not doing his/her fair share of the work. (Evident in reflection)	The workload was not divided OR one member viewed as not doing their fair share of the work. (Evident in reflection)

We will use a mapping of the letters of the alphabet with the numbers 0 to 25

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

1. Use a linear function (y = *m*x + *b*) for your encryption:

   My assigned slopes are _____ and _____.

2. Using the mapping of the alphabet, each letter is assigned a number (see above). Use this as the x-value in your equation. To find the letters for the cryptic phrase, you must add or subtract 26 from the calculated y-value until you get a number between 0 and 25. Then match that number to the corresponding letter from above. Do this for each of your assigned slopes (you may choose your y-intercept value).

Equation: _____

Original	x	y	New
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			
K			
L			
M			

Original	x	y	New
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

Equation: _____

Original	x	y	New
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			
K			
L			
M			

Original	x	y	New
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

3. Which of the slopes you have investigated will make the message possible to decode with a function? How do you know?

In order for the decoding equation to be a function, you need to be careful about the coding equation you use. We will use a linear function and choose a slope which will produce a one-to-one function.

List of slopes which work:

List of slope to avoid:

In general, what is the relationship with the slopes that work to 26?

My coding equation will be _____

Original	x	y	New
A			
B			
C			
D			
E			
F			
G			
H			
I			
J			
K			
L			
M			

Original	x	y	New
N			
O			
P			
Q			
R			
S			
T			
U			
V			
W			
X			
Y			
Z			

My coded quote:

Copy this cryptogram on a separate sheet of paper and give it to your partner!

Given a linear relationship between two variables, what is its inverse?

REVIEW: Find the equation for a line between the points (8, 5) and (12, 8)

When investigating a new number system, a question to explore is: does every number have a multiplicative inverse?

> ***Multiplicative inverse:*** The number which you multiply by to get a product of 1.

Which numbers have a multiplicative inverse mod 26?

Find the multiplicative inverse (mod 26) for each of the possible numbers which could have been used for m.

m	$\frac{1}{m}$ or m^{-1}
1	
3	
5	
7	
9	
11	
15	
17	
19	
21	
23	
25	

Redo the review problem from above in mod 26.

What to remember when writing your decoding equation:

$$slope = \frac{\text{distance apart of original letters}}{\text{distance apart of the coded letters}}$$

If we call the distance between the two letters d, then the gcd(d, 26) = 1.

EXAMPLE: TNQK CHIFJ

Pick two letters in the cryptogram to decode.

_____ → _____ and _____ → _____

Write these as ordered pairs using the mapping of letters to the numbers 0 to 25.

(,) and (,)

Find the decoding equation.

Try this decoding equation on an entire word. If it doesn't work, then *start over*. Keep track of all your work.