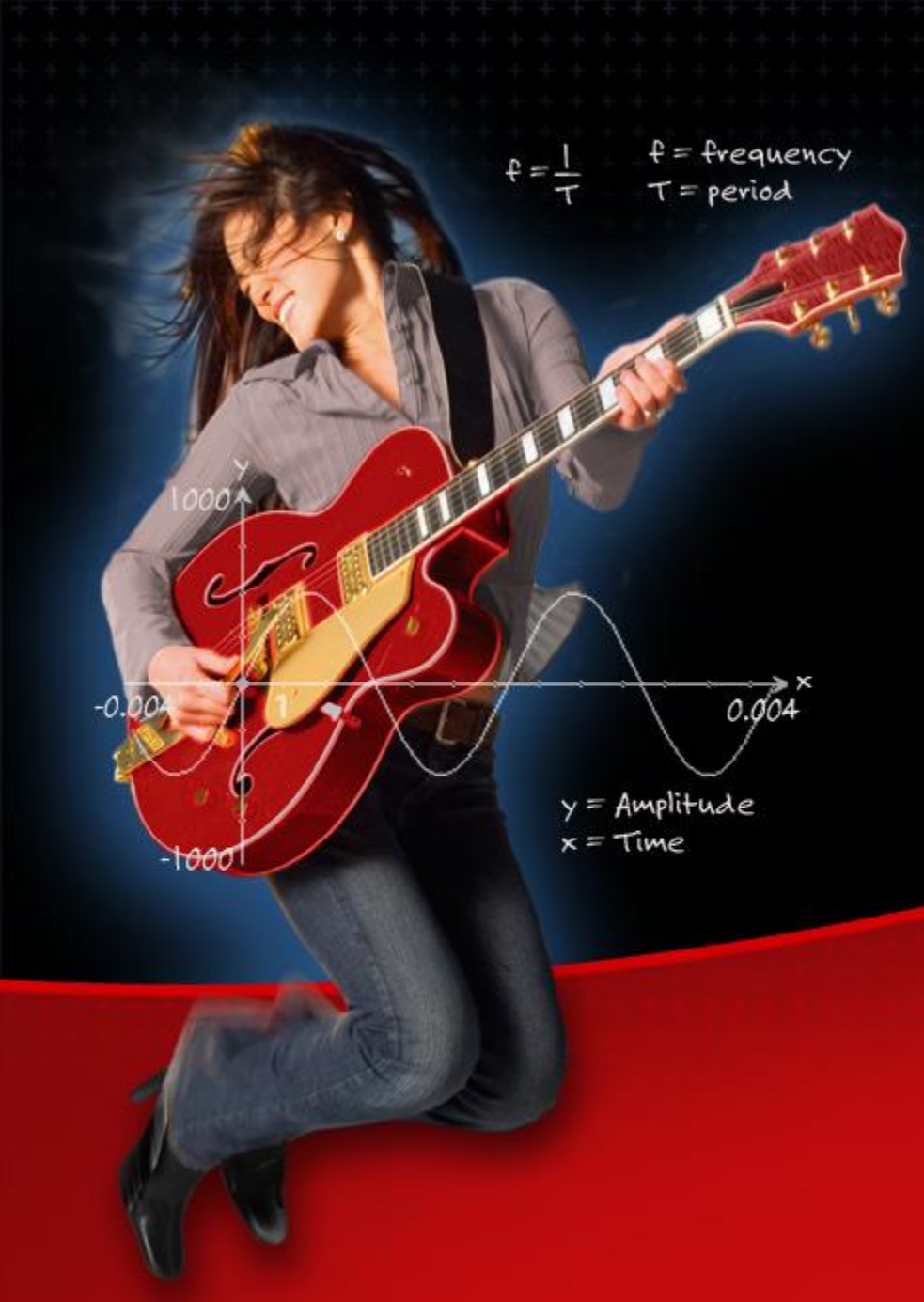
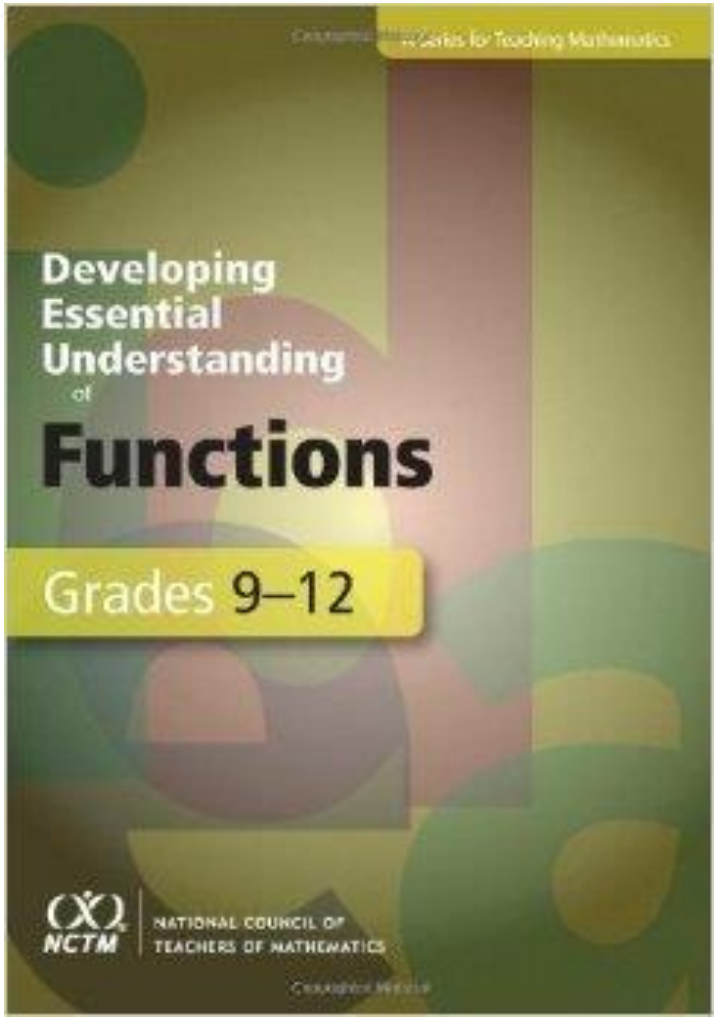


Cryptography Using Linear Functions and Their Inverses

Kara Leaman
kara.leaman11@gmail.com

Ann Schlemper
aschlemper@ccis.edu



1. The Function Concept
2. Co-variation and Rate of Change
3. Families of Functions
4. Combining and Transforming Functions
5. Multiple Representations of Functions

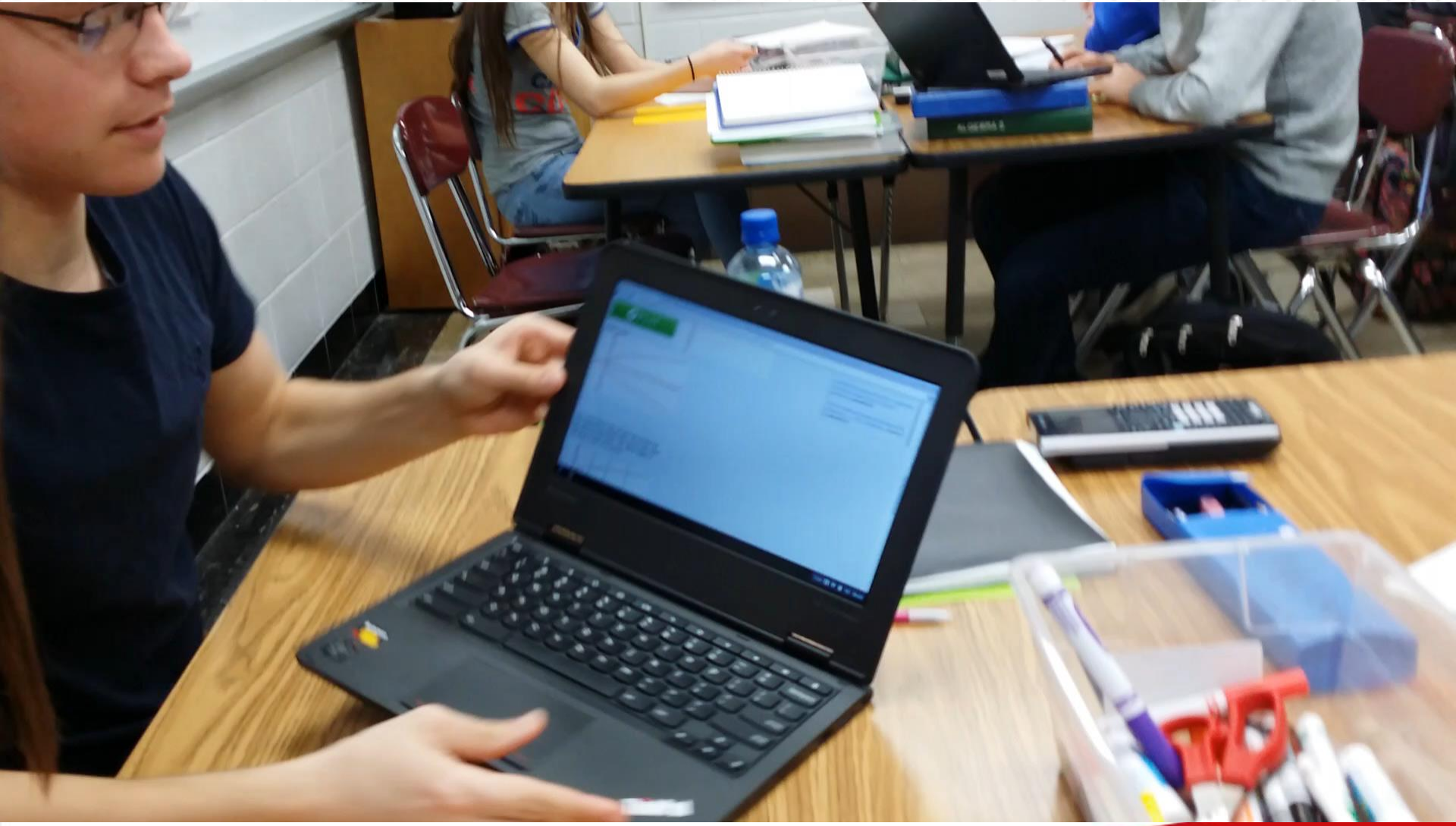
Big Idea 1. The function concept

Essential Understanding 1*a*. Functions are single-valued mappings from one set—the *domain* of the function—to another—its *range*.

Essential Understanding 1*b*. Functions apply to a wide range of situations. They do not have to be described by any specific expressions or follow a regular pattern. They apply to cases other than those of "continuous variation." For example, sequences are functions.

Essential Understanding 1c. The domain and range of functions do not have to be numbers. For example, 2-by-2 matrices can be viewed as representing functions whose domain and range are a two-dimensional vector space.

Algebra 2 Students' Ideas about the Definition of a Function



Calculus Students' Ideas About Inverse Functions

Student 1:

The inverse of a function is taking our outputs and finding the input.

The inverse of a function is the opposite graph of the function graph.

Student 2:

I think you switch the x and y and then solve to find the new function (inverse function). I'm not sure graphically how it looks.

Student 3:

To find the inverse of a function, you switch the x and the y and solve for y. The domains are somehow related?

Using Modulus

$$a \equiv b \bmod m \quad \Leftrightarrow$$

$$m \mid (b - a) \quad \Leftrightarrow$$

b and a have the same remainder when divided by m

$$111 \equiv 7 \bmod 26$$

$$111 \equiv 33 \bmod 26$$

$$38 \equiv 12 \bmod 26$$

$$38 \equiv 194 \bmod 26$$

Cryptography using Linear Functions and Mod 26

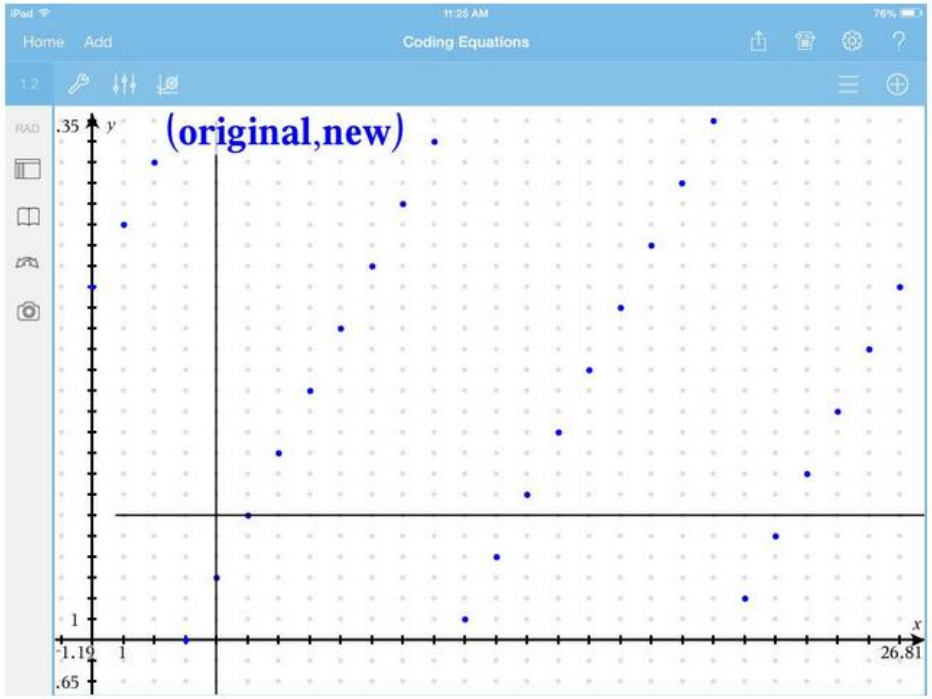
A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

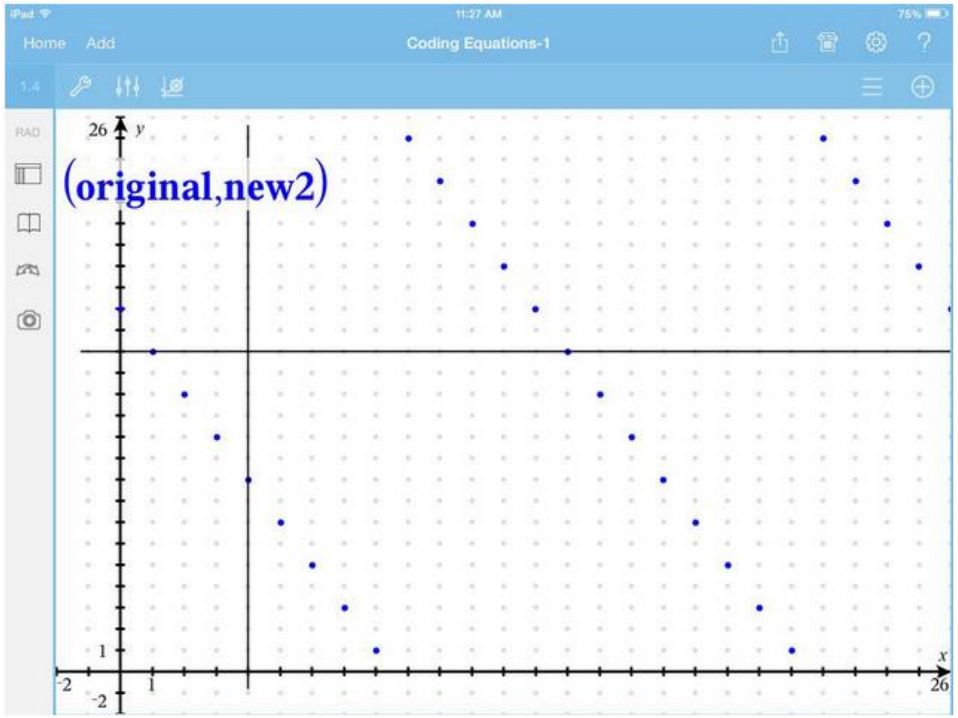
Equation: _____

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			

Coding Equations



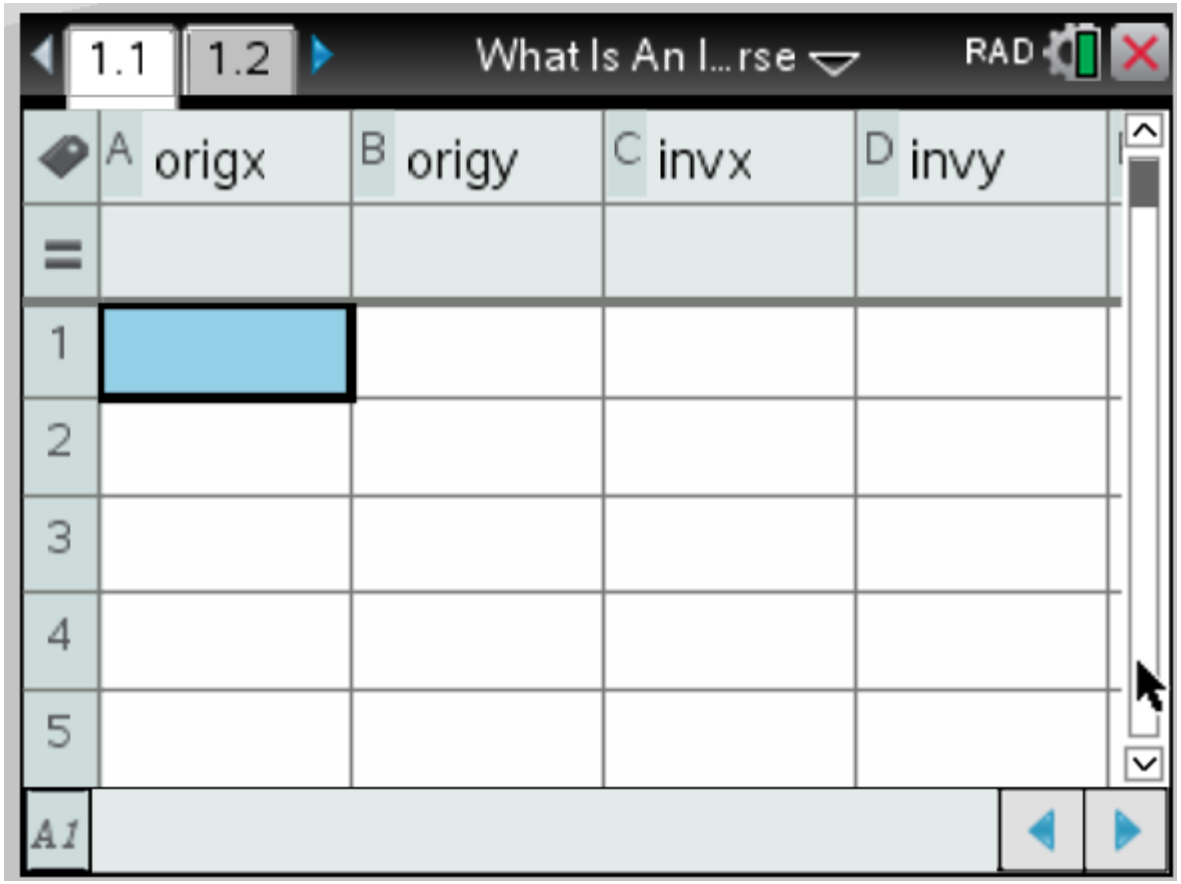


Coding a Cryptogram

$$y = 5x - 12$$

Message:
NCTM BOSTON

Inverse of a Linear Function
(The reflection across the line y = x)



What is division in Mod 26?

$$\frac{3}{7} = 3 \cdot 7^{-1} \equiv 3 \cdot 15 \equiv 19$$

$$\frac{10}{6} = 10 \cdot 6^{-1}$$

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}
1	9	21	15	3	19

15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
7	23	11	5	17	25

Decoding a Cryptogram

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.

What letter combinations work and which don't?... And why?

T	N	Q	K
M	A		

C	H	I	F	J

Then these can be written as (19, 12) and (13, 0) and then the slope would be

$$m = \frac{12-0}{19-13} = \frac{12}{6} = 12 \cdot 6^{-1} \equiv ?$$

What letter combinations work and which don't?... And why?

T	N	Q	K
M			

C	H	I	F	J
R				

Then these can be written as (19, 12) and (2, 17) and then the slope would be

$$m = \frac{12-17}{19-2} = \frac{-5}{17} =$$

$$-5 \cdot 17^{-1} = 21 \cdot 17^{-1}$$

$$\equiv 21 \cdot 23 \equiv 15$$

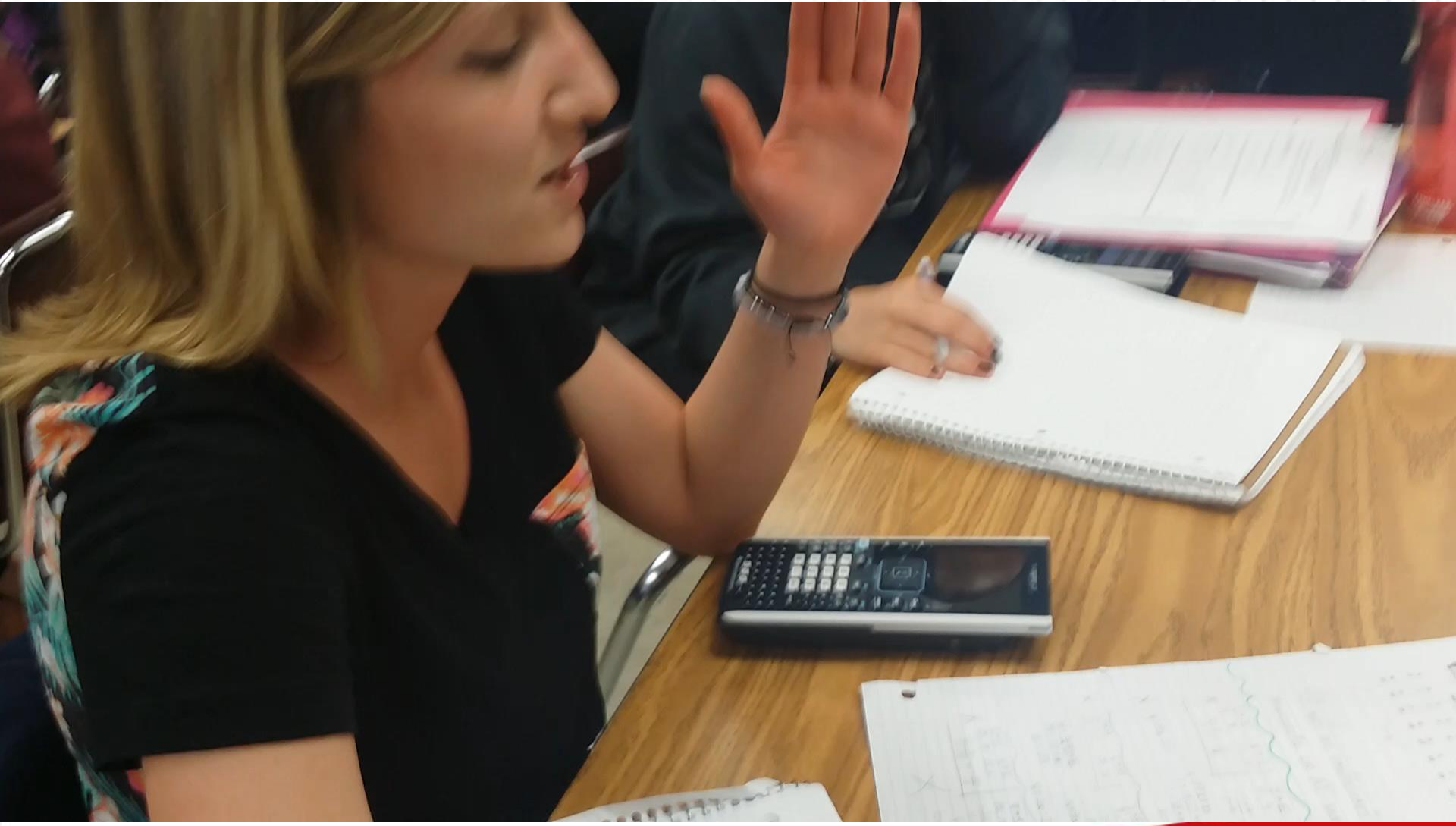
$$y - 12 = 15(x - 19)$$

$$y - 12 = 15x - 15 \cdot 19$$

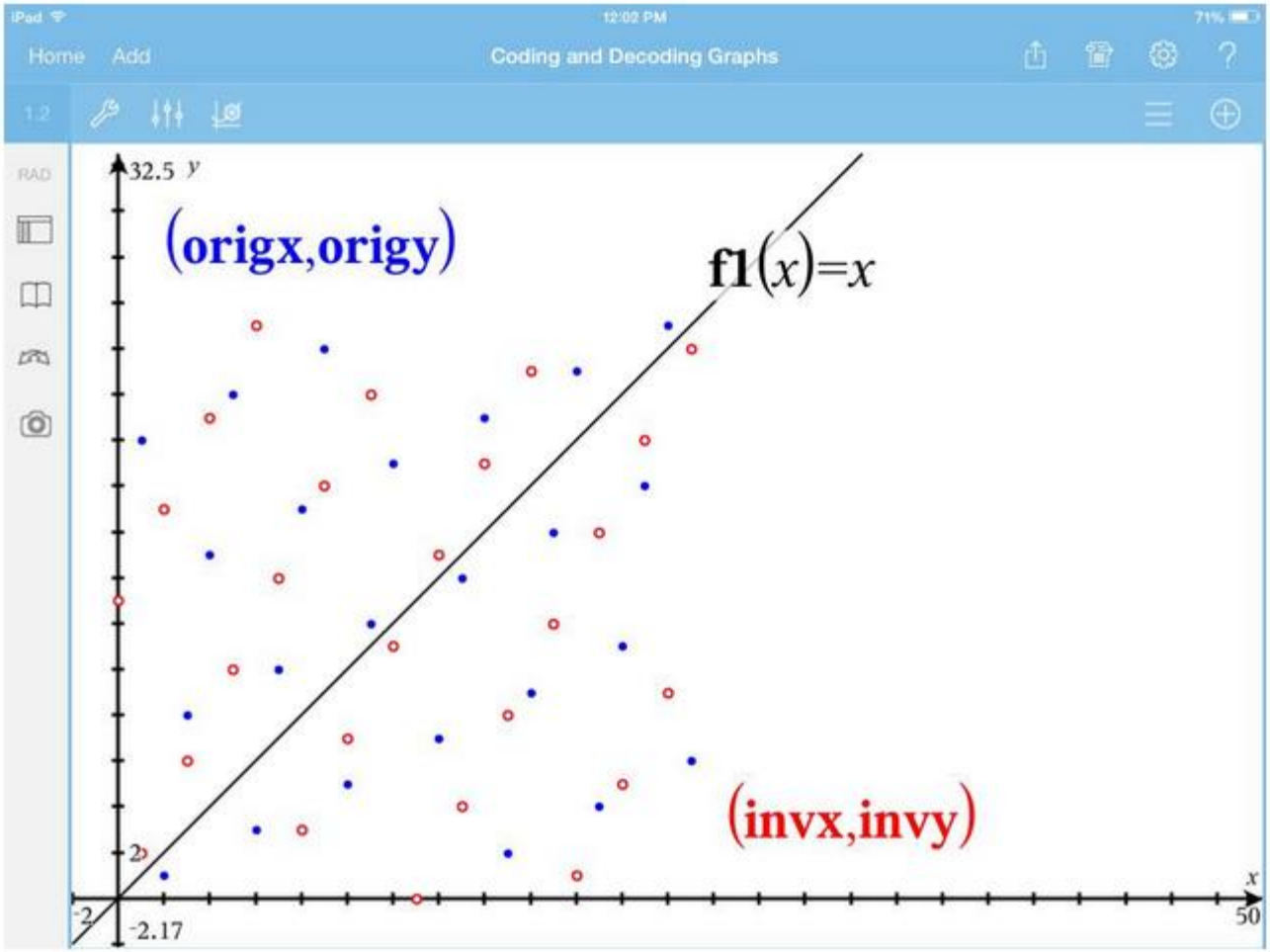
$$y - 12 = 15x + 1$$

$$y = 15x + 13$$

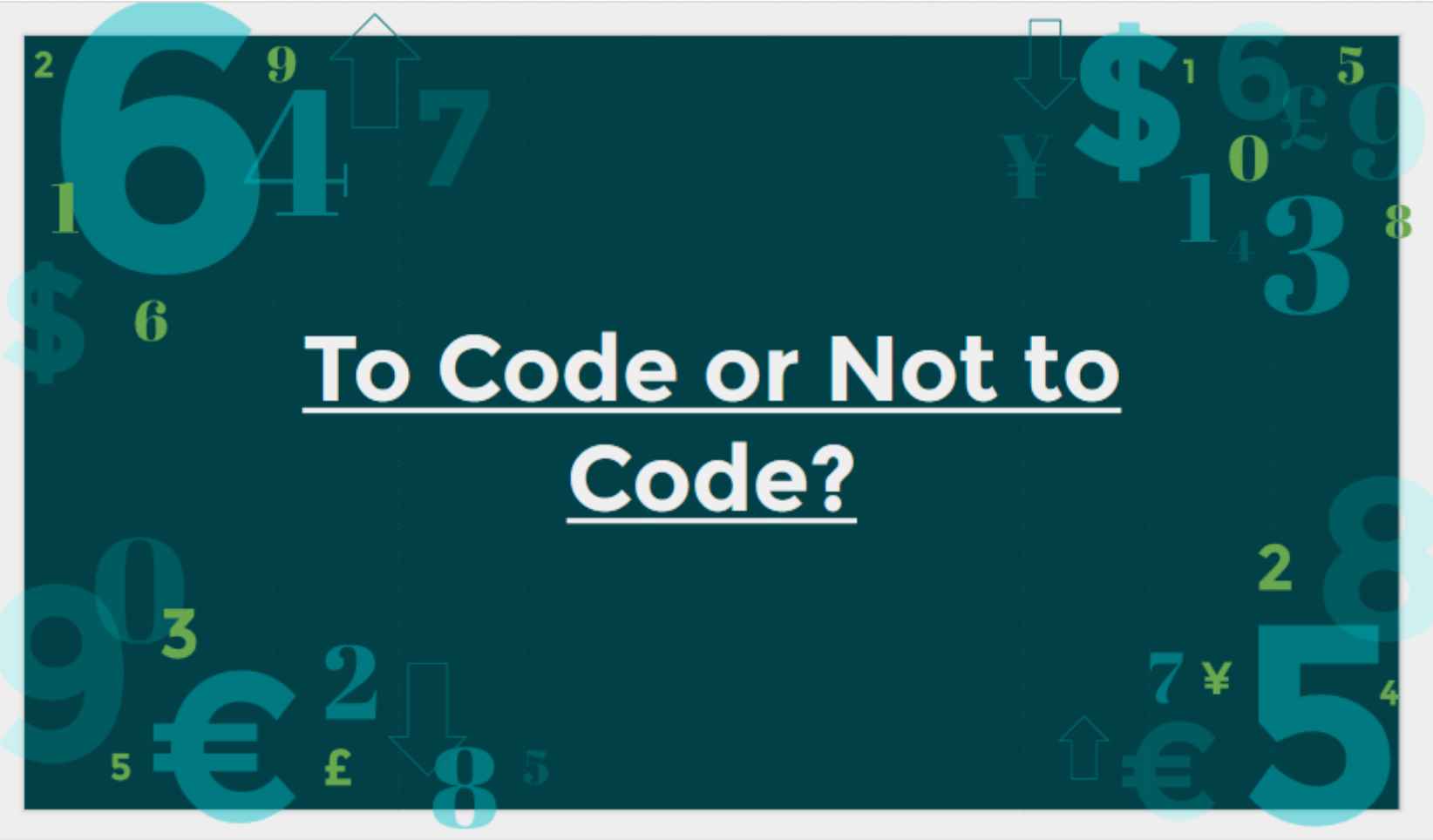
Students Efforts at Decoding Each Others Messages



Coding and Decoding Graphs



An Example of Two Students' Projects



What did students learn about functions?

Is the relation a function? State yes or no, then provide a reason for your answer. {(2, 4), (2, 6), (-1, 3), (9, 2)}

no, because if you graph the points, two of them will be on the same vertical line, and if it was a function, they wouldn't be on the same vertical line.

no because in (2,4) & (2,6) there are 2 possibilities for the point. like saying 2 is equal to 4 and 2.

This is not a function because there are 2 different y-values for one x-value.

no, it is not a function because there are two of the same x-values. eg: (2,4) (2,6)

What did students learn about inverse functions?

Are the functions f(x) = -3x and g(x) = 3x inverse functions? State yes or no, and provide a reason for your answer.

no

When you switch the x & y of g(x) = 3x, it does not equal -3x.

no, they aren't because they aren't symetric to y=x

no because the first coordinate of y=-3x is (1,-3) that said the inverse should be (-3,1) and y=3x first coordinate is (1,3)

no

3(-3x) = -9x

Student Reflections on Cryptography

Student 1:
I do think this project helped me understand the idea and concept of inverse functions. It also brought to my eyes this whole new world of math i never had any idea about. I honestly didn’t know that math was involved in coding and how much cryptography actually affects our lives today.

Student Reflections on Cryptography

Student 2: Overall I found this project both challenging and intriguing. I loved the idea of decoding a secret message and finding out what it is. I also loved this project because it has to do with the field I want to go into as a career. Although this wasn't computer code dealing with languages and softwares of computers it very much applies to those areas and has excited me for the future.