Cryptography: Keeping Secrets Using Algebra and Geometry

André Mathurin
Bellarmine College Preparatory (San Jose, CA)

With the increasing reliance on e-mail and texting, how can mathematics help ensure that these communications remain private? Come learn ways to do so and get ideas for engaging students in the basic ideas of cryptography within the context of algebra and geometry topics.

Contact & Resource Information

amathurin@bcp.org

http://tinyurl.com/Crypto-NCTM2014

Friday, April 11, 2014
01:00 PM - 02:15 PM
203/204/205 Convention Center

Preliminaries

- Goals
- Format
- Disclaimers

Preliminaries

- Goals
  - ✓ *Spark Ideas for Teaching Functions*
  - ✓ *Introduce Cryptography using Algebra & Geometry*

Understand the concept of a function and use function notation.

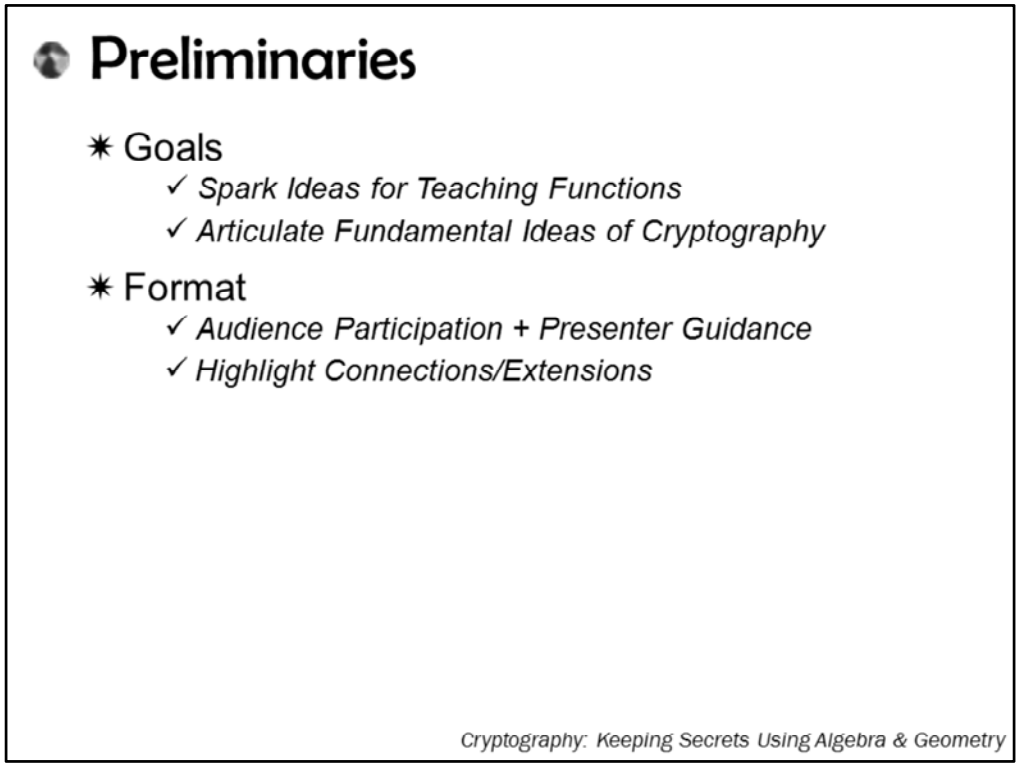
CCSS.MATH.CONTENT.HSF.IF.A.1

Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then $f(x)$ denotes the output of f corresponding to the input x. The graph of f is the graph of the equation $y = f(x)$.

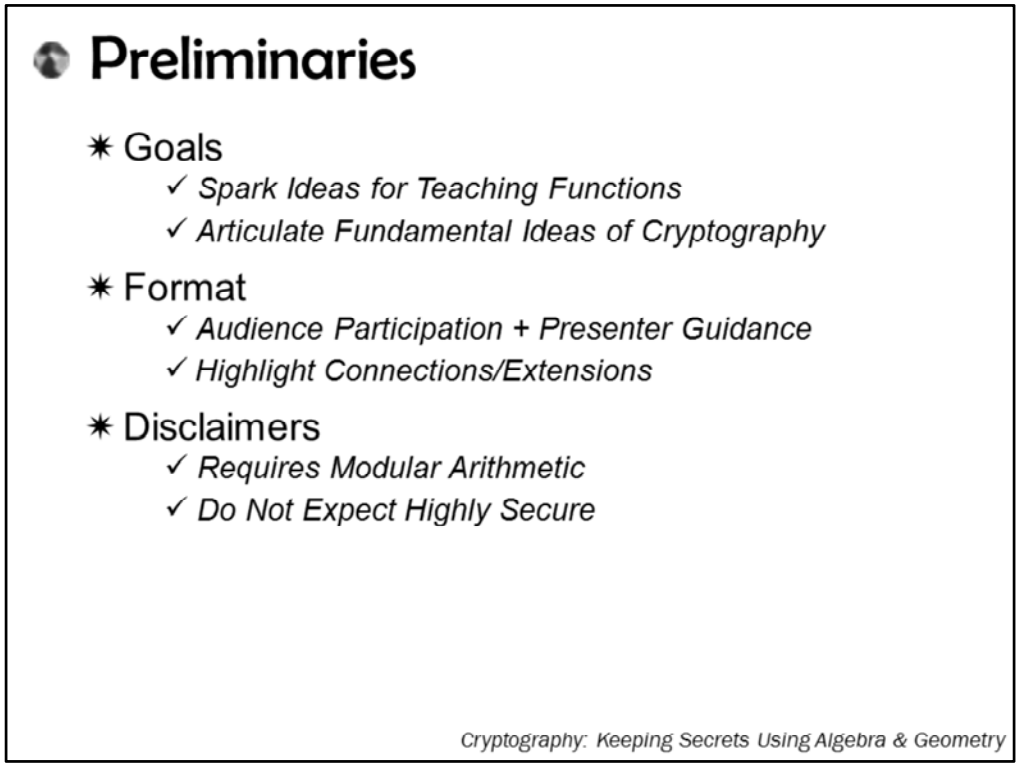
CCSS.MATH.CONTENT.HSF.IF.A.2

Use function notation, evaluate functions for inputs in their domains, and interpret statements that use function notation in terms of a context.

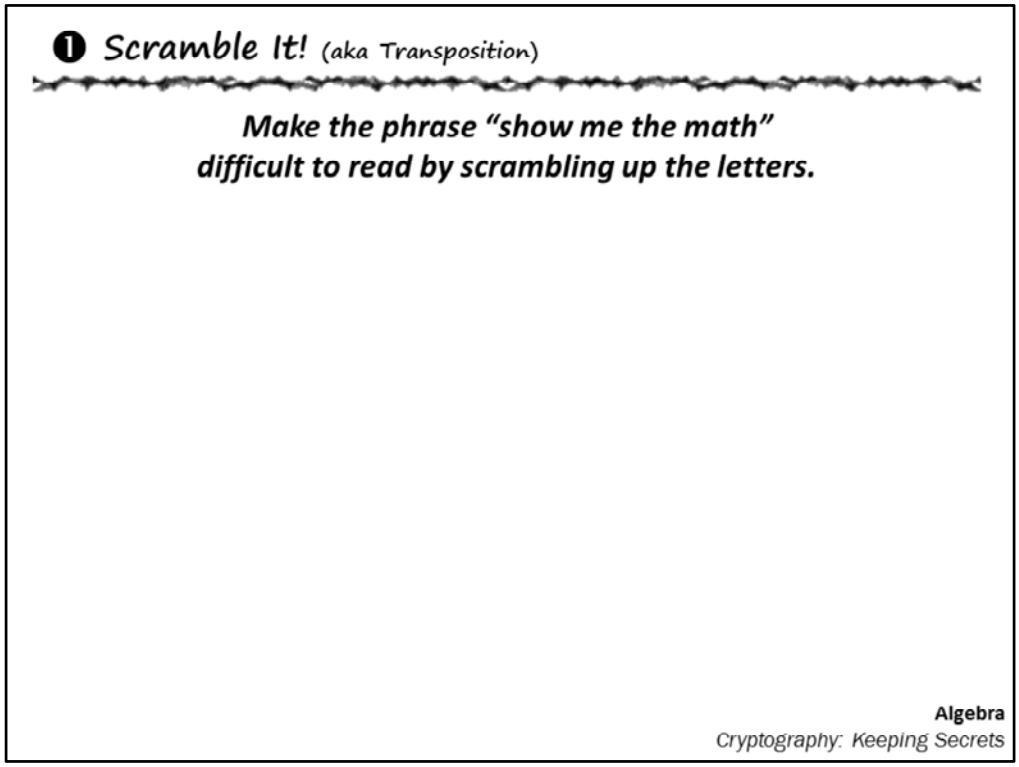
Focus on Functions
adjust as you desire.



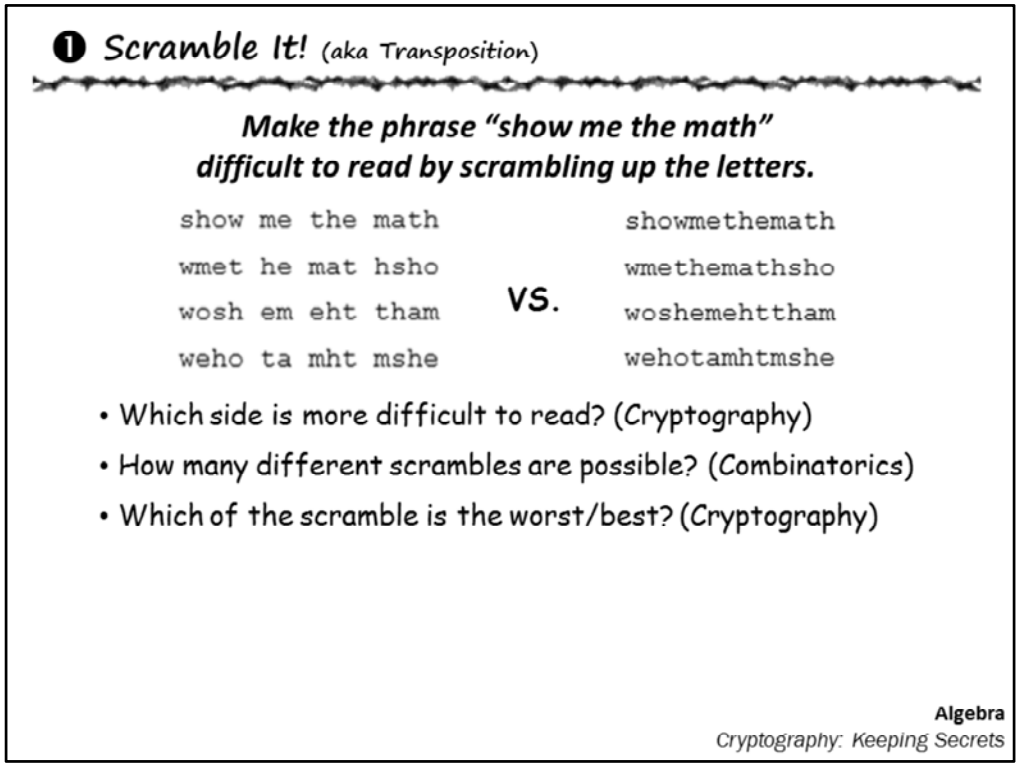
Activities are not designed to fit into the existing Algebra, Geometry, Precalculus structure. Could be used as enrichment, warm-ups, extra credit, etc.



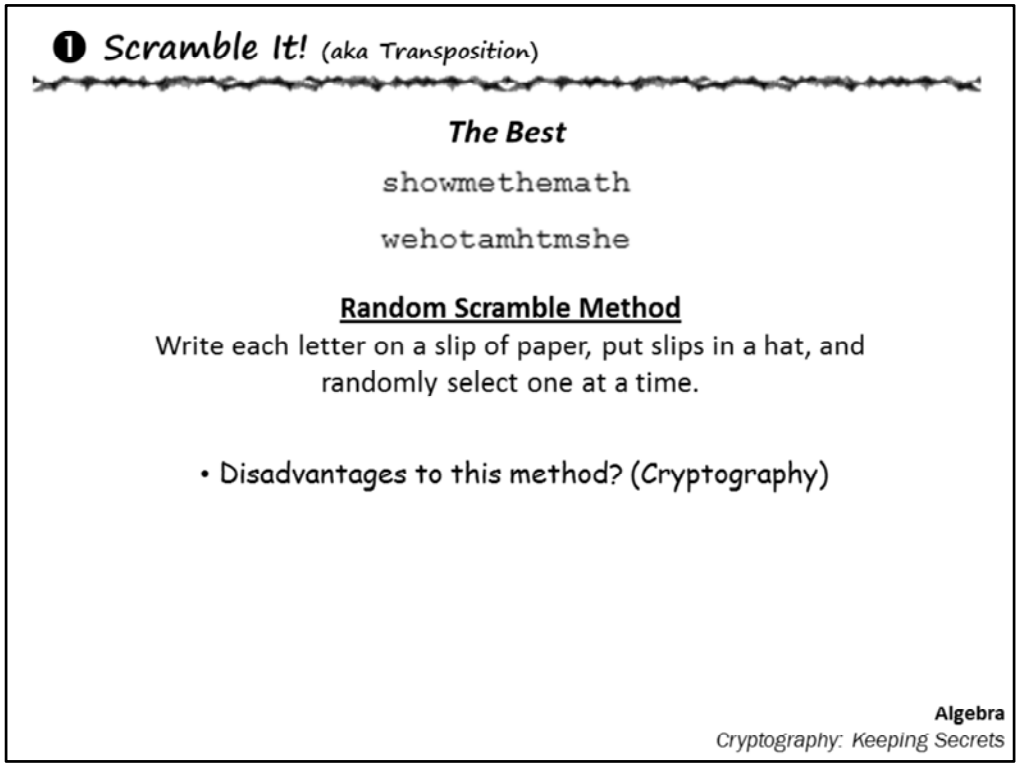
Modular Arithmetic basics only – will highlight extensions
Basic Elements of Cryptography – will suggest areas for more discussion



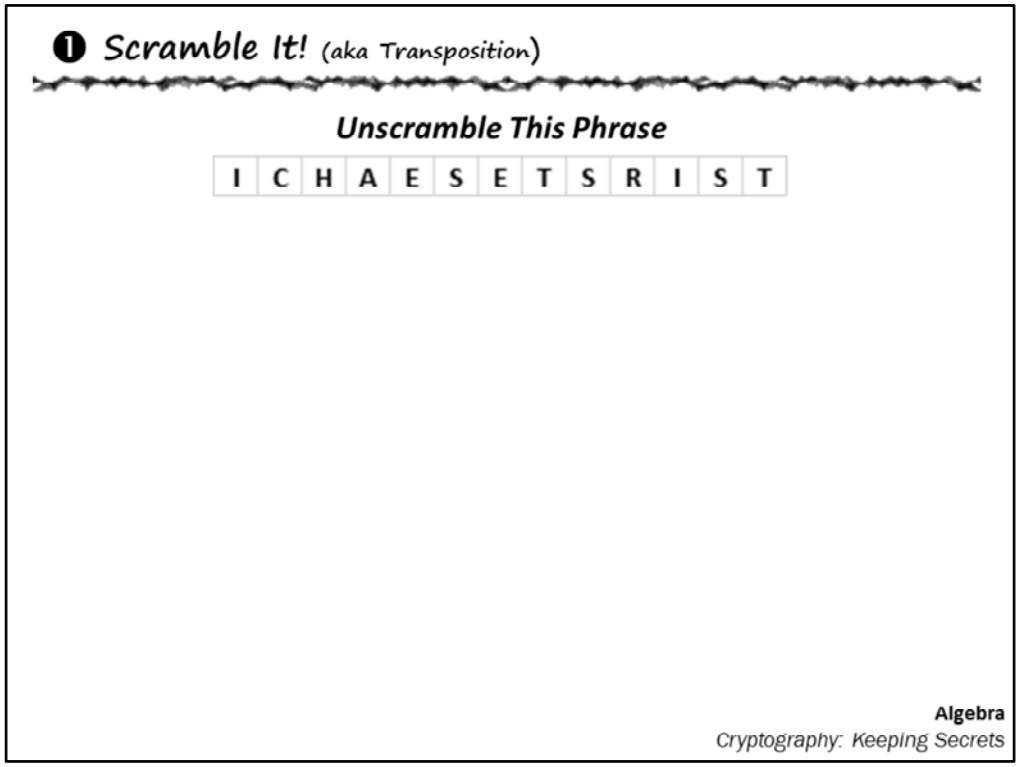
Give participants a minute to come up with a scramble.
Then give them a minute to compare their scramble with others.



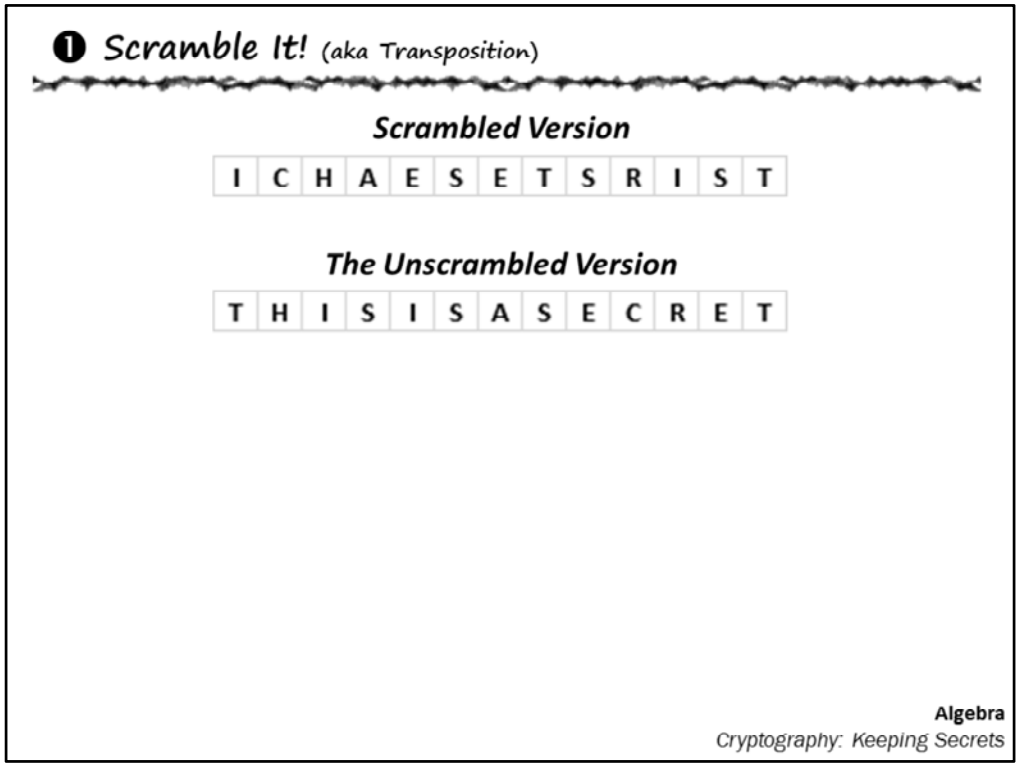
More difficult to read? Right side because no word grouping / hard to see the words
How many different scramble possible? 129,729,600
Which is the worst? Second because just shifting
So if we throw out "bad" scrambles, how many scrambles are we left with?
Which is the best? hopefully the last one will be the winner of the best!



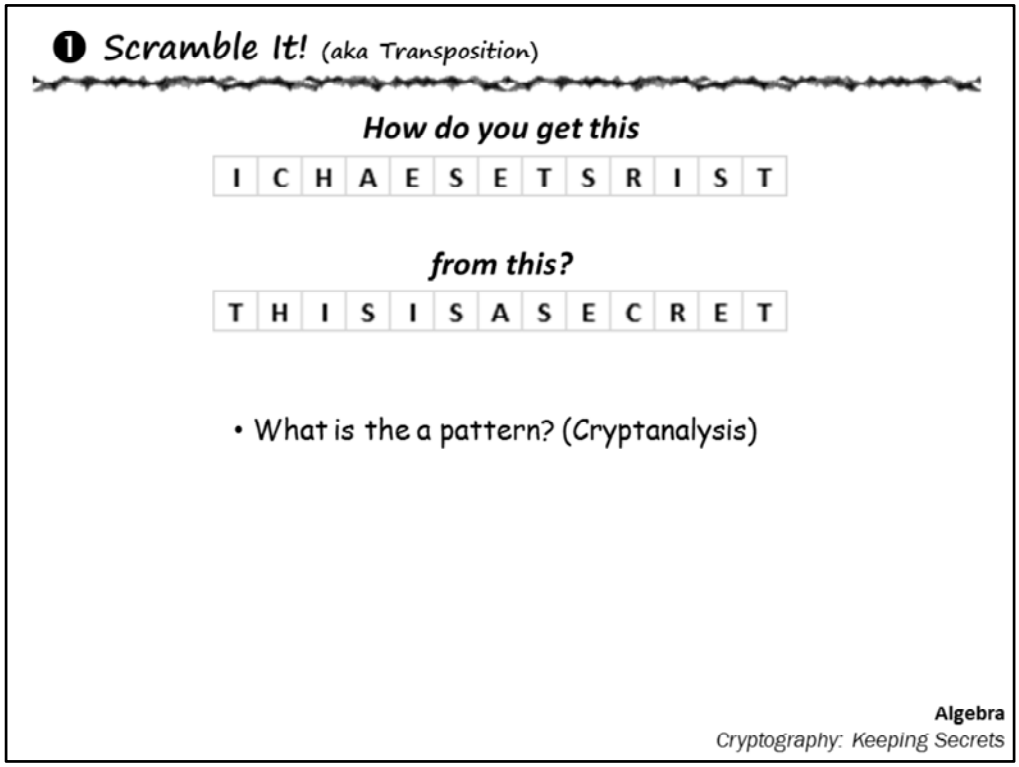
Takes time to write all the slips of paper and select one at a time – especially if the message is long.
Unless you know what the original unscrambled message was, good luck at unscrambling.
The process for scrambling is not reversible UNLESS you've written down the exact scrambling order.



Give participants 3 minutes to attempt to unscramble – either work alone or collaboratively.



Not knowing
(1) the word grouping breaks (number of words)
(2) context
makes this task challenging.



There is a pattern – it's based on Modular Arithmetic
Hint: Look for unique characters
Now that we know this patter, could do it this way, but as the message gets longer, counting becomes more tedious
What about sharing the wealth? Create a system where people can work independently and contribute to a solution.
Need for a precise description of this system – Let's get to ALGEBRA and functions to do this.

❶ Scramble It! (aka Transposition)

Modular Scramble Method

creates a pseudo-random "mixing up" of the phrase

Define the function $Char(n)$ as the character that appears in the n^{th} position of the message.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$Char(n)$	T	H	I	S	I	S	A	S	E	C	R	E	T

$Domain = \{1,2,3,4,5,6,7,8,9,10,11,12,13\}$

$Range = \{A, C, E, H, I, R, S, T\}$

example: $Char(9) = E$

Algebra

Cryptography: Keeping Secrets

Is the Char function one-to-one?
Is there an inverse function for Char?

❶ Scramble It! (aka Transposition)

Modular Scramble Method

creates a pseudo-random "mixing up" of the phrase

Define the function $ModMixup(n)$ as a scramble of the position values n.

$ModMixup$

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$5n \ (mod\ 13)$	5	10	2	7	12	4	9	1	6	11	3	8	13

$Domain = \{1,2,3,4,5,6,7,8,9,10,11,12,13\}$

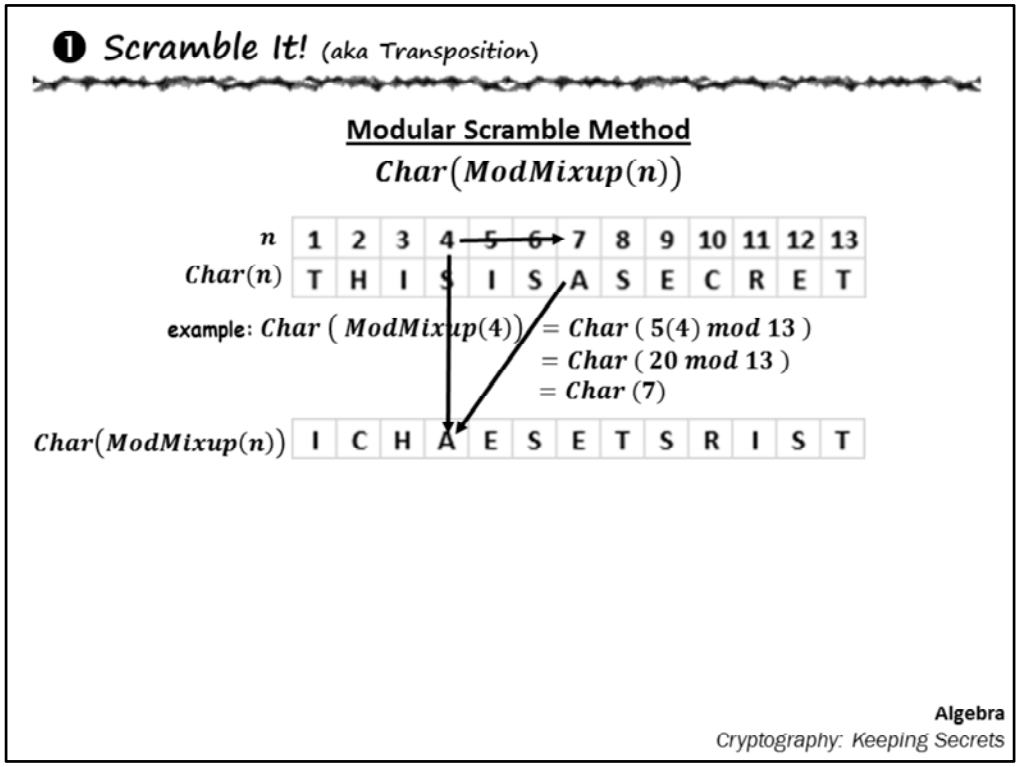
$Range = \{1,2,3,4,5,6,7,8,9,10,11,12,13\}$

example: $ModMixup(5) = 12$

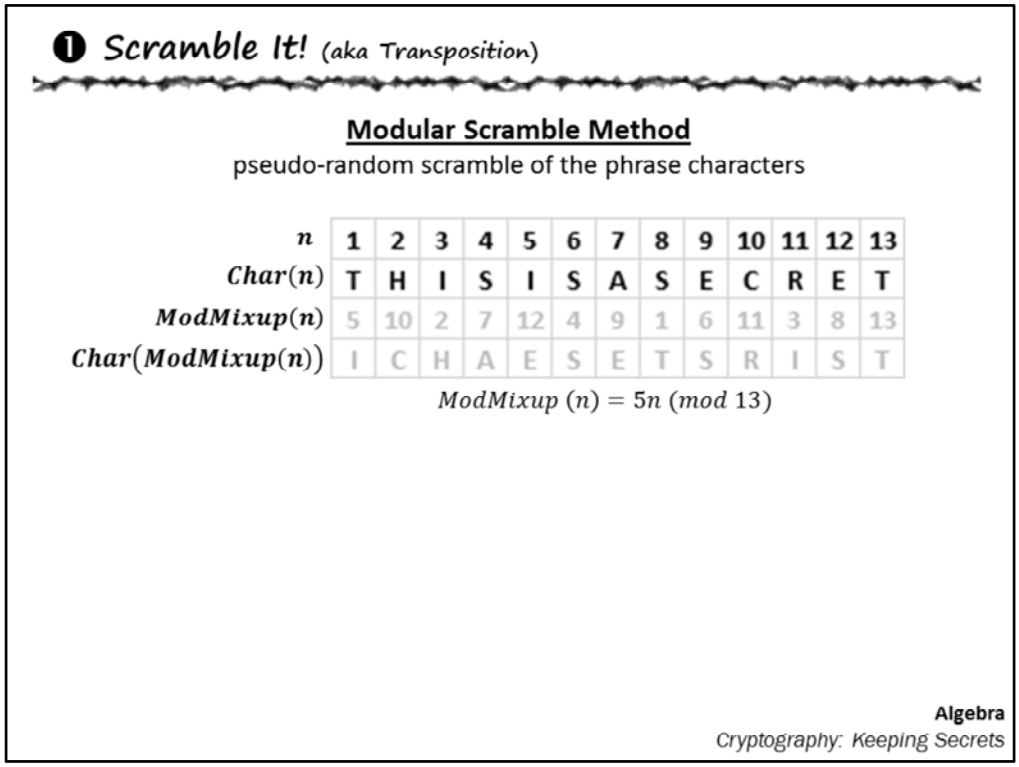
Algebra

Cryptography: Keeping Secrets

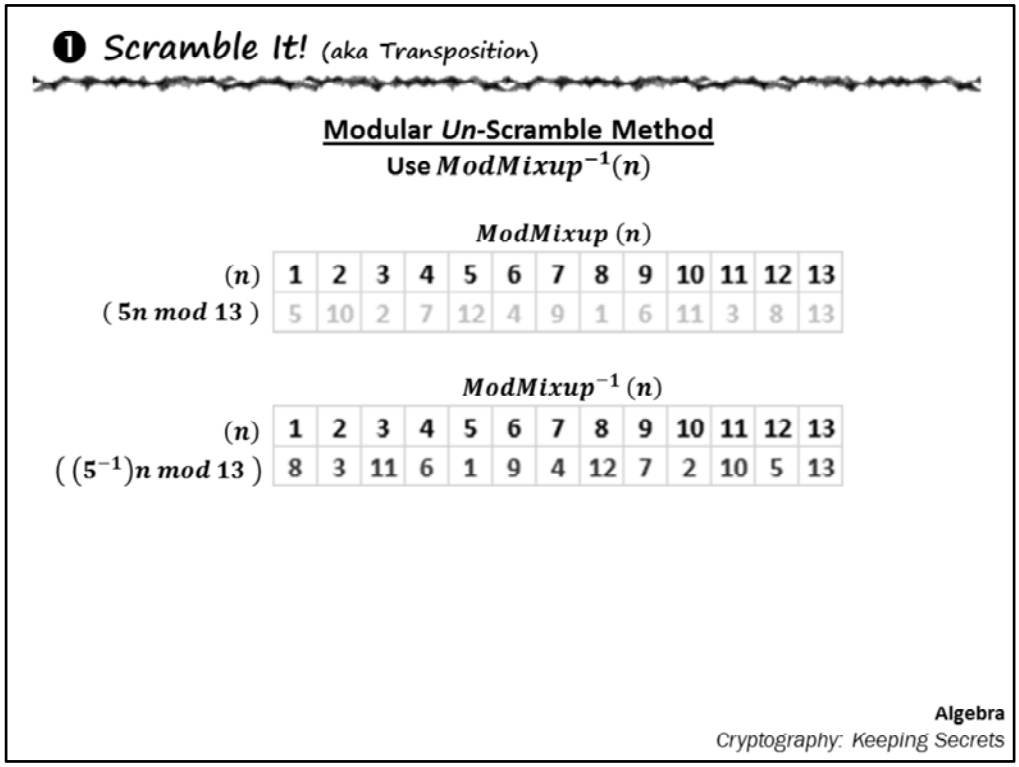
What are the conditions for the ModMixup function? (one-to-one, inverse)
Necessary – one-to-one/why?



What are the conditions for the mixup function? (one-to-one, inverse)
Why iNecessary – one-to-one/why?



What are the conditions for the mixup function? (one-to-one, inverse)
Necessary – one-to-one/why?



Great aside for discussion of the choice of coefficients & relationship to mod
connection to 1-to-1 functions because of need for the inverse function to exist
Picked 5 because easy to multiply and makes it easy to find the inverse of 5
Side note about notation of raised to the negative 1 power…here is my soapbox opportunity

❶ Scramble It! (aka Transposition)

Modular *Un*-Scramble Method

$$Char\left(ModMixup^{-1}(n) \right)$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$Char(n)$	I	C	H	A	E	S	E	T	S	R	I	S	T

example: $Char\left(ModMixup^{-1}(4)\right) = Char\,(\,8(4)\ mod\ 13\,)$

$= Char\,(\,32\ mod\ 13\,)$

$= Char\,(6)$

$Char\left(ModMixup^{-1}(n)\right)$	T	H	I	S	I	S	A	S	E	C	R	E	T

❶ Scramble It! (aka Transposition)

Modular *Un*-Scramble Method

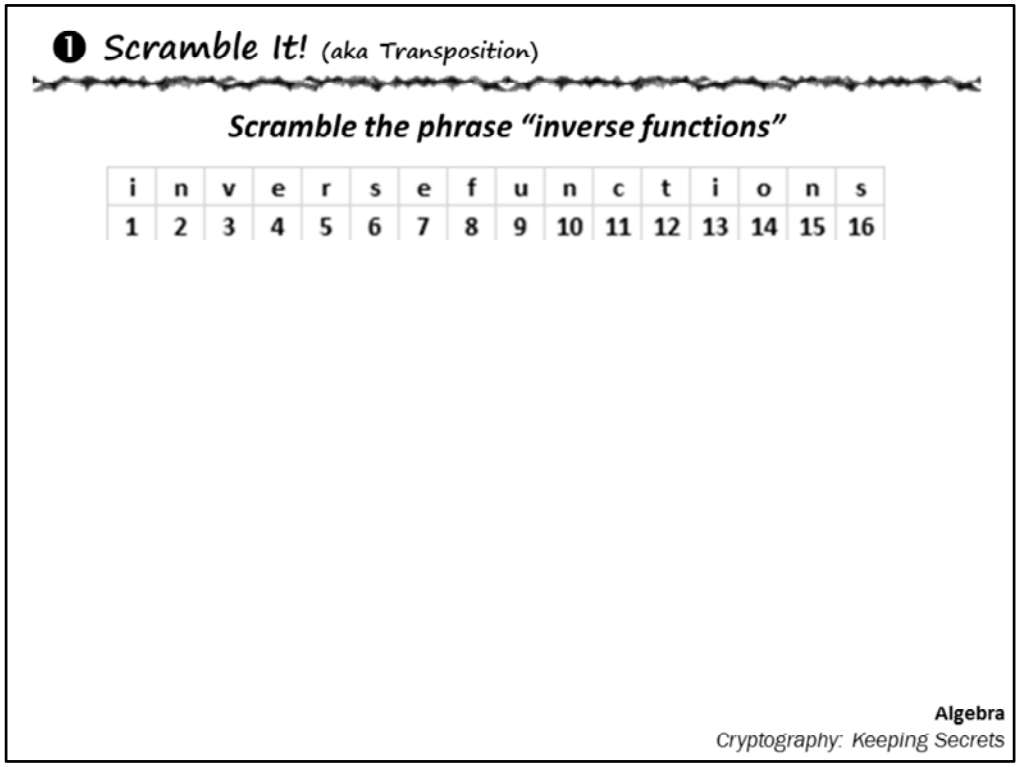
$$Char\left(ModMixup^{-1}(n) \right)$$

(n)	1	2	3	4	5	6	7	8	9	10	11	12	13
$Char\ (n)$	I	C	H	A	E	S	E	T	S	R	I	S	T
$ModMixup^{-1}(n)$	8	3	11	6	1	9	4	12	7	2	10	5	13
$Char\ (\ ModMixup^{-1}(n)\ )$	T	H	I	S	I	S	A	S	E	C	R	E	T

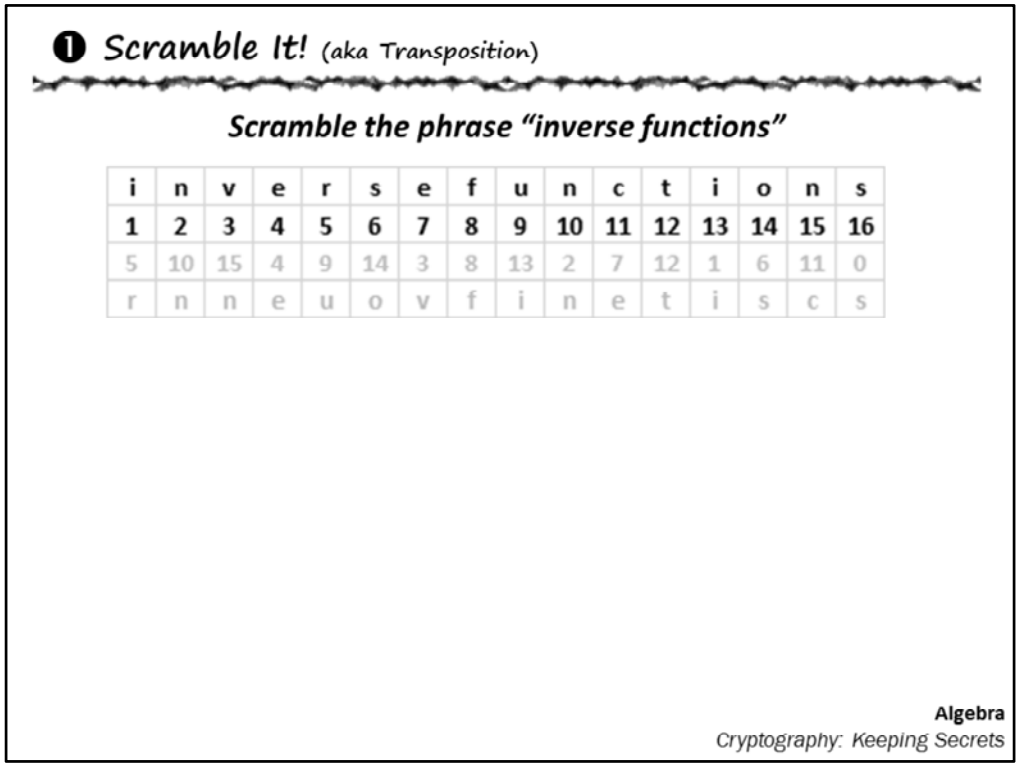
$$ModMixup^{-1}(n) = 8n\ (mod\ 13)$$

Algebra
Cryptography: Keeping Secrets

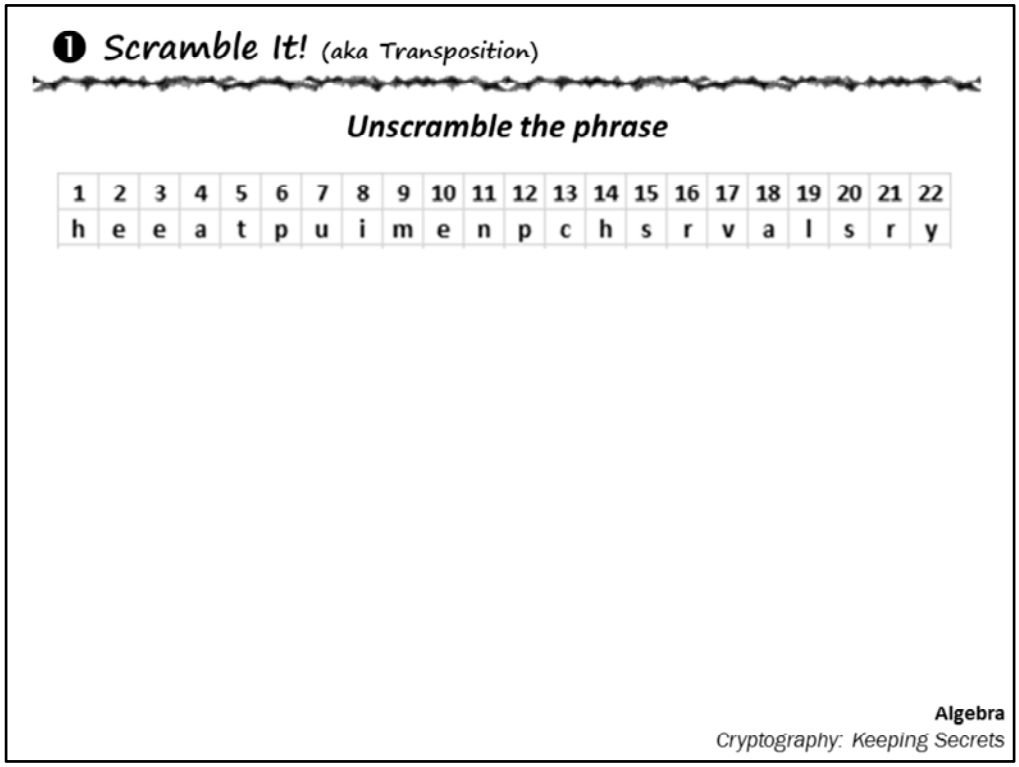
What are the conditions for the mixup function? (one-to-one, inverse)
Necessary – one-to-one/why?



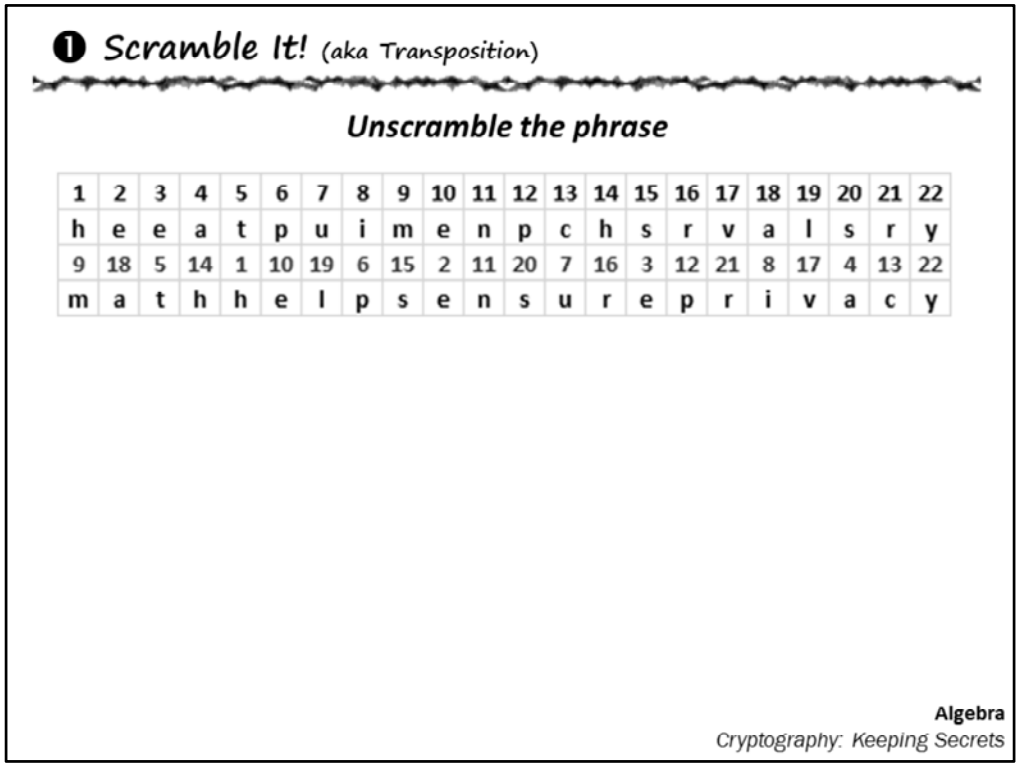
Give participants a minute to come up with a scramble.
Then give them a minute to compare their scramble with others.



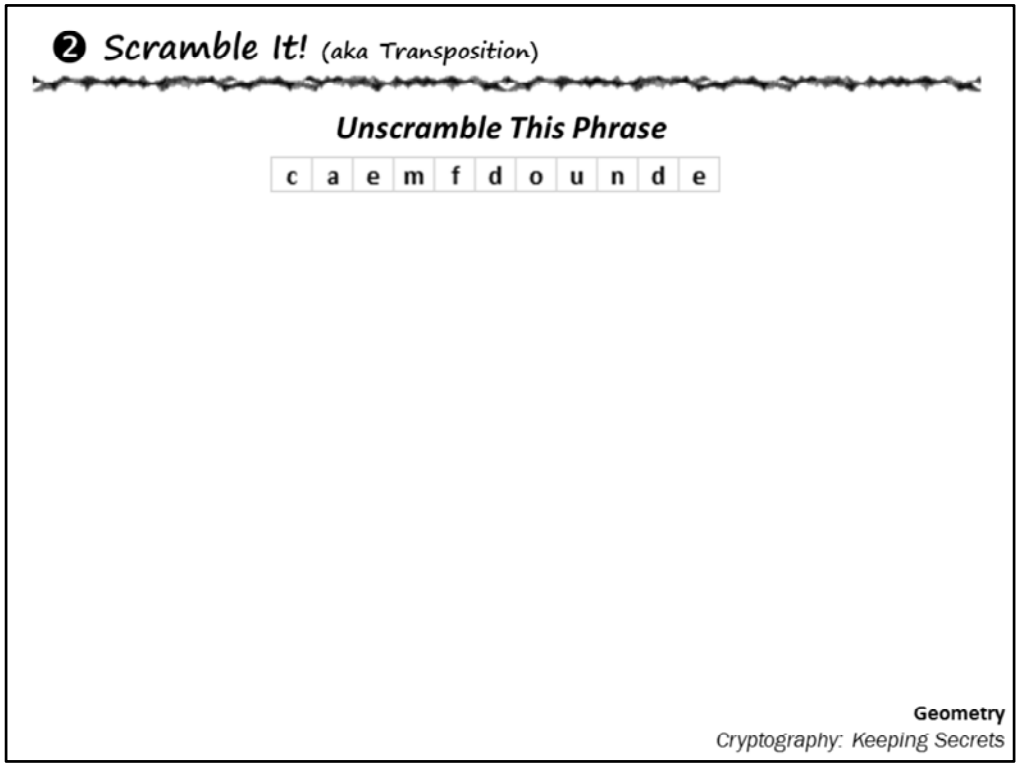
Give participants a minute to come up with a scramble.
Then give them a minute to compare their scramble with others.



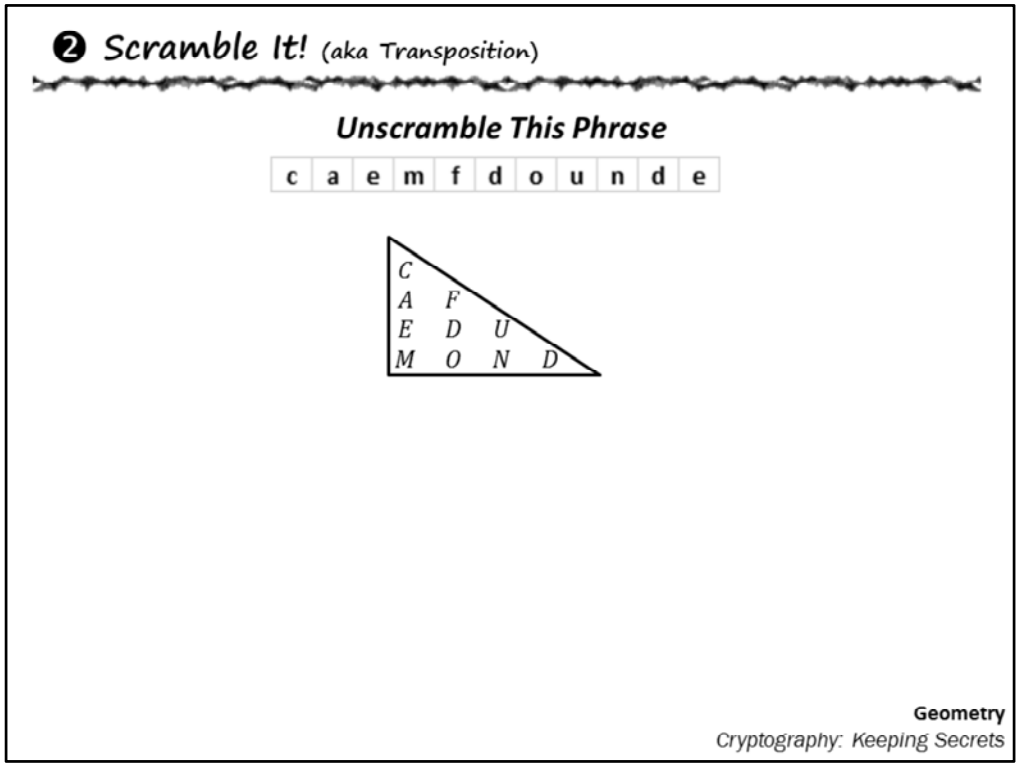
Give participants a minute to come up with a scramble.
Then give them a minute to compare their scramble with others.



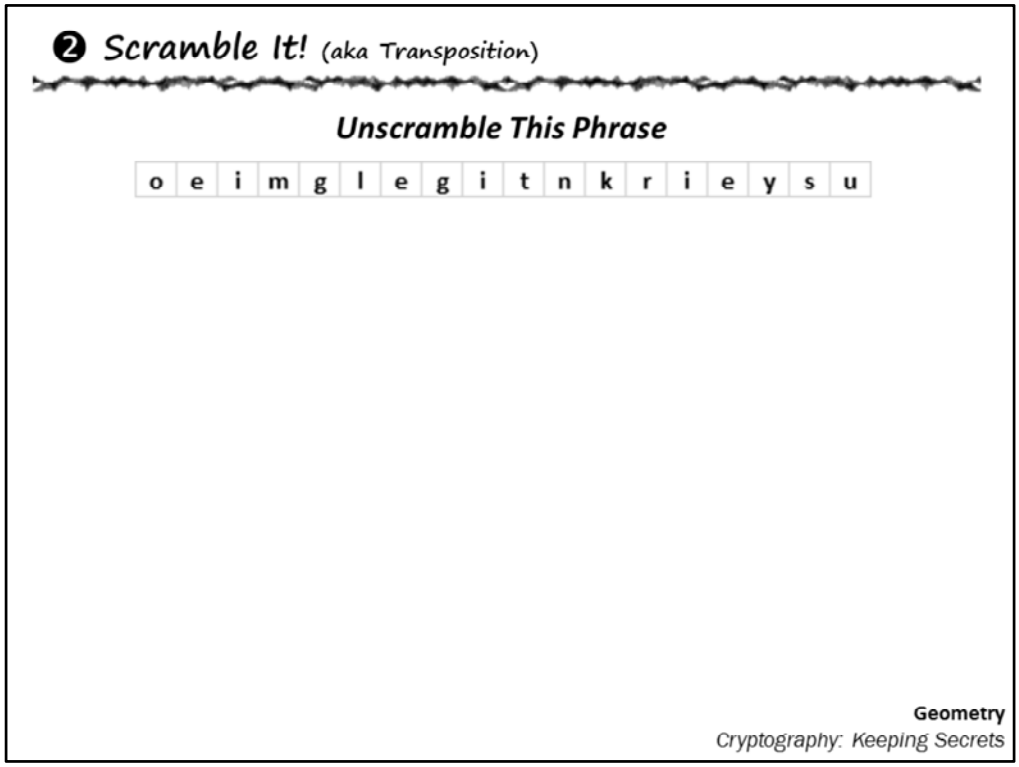
Give participants a minute to come up with a scramble.
Then give them a minute to compare their scramble with others.



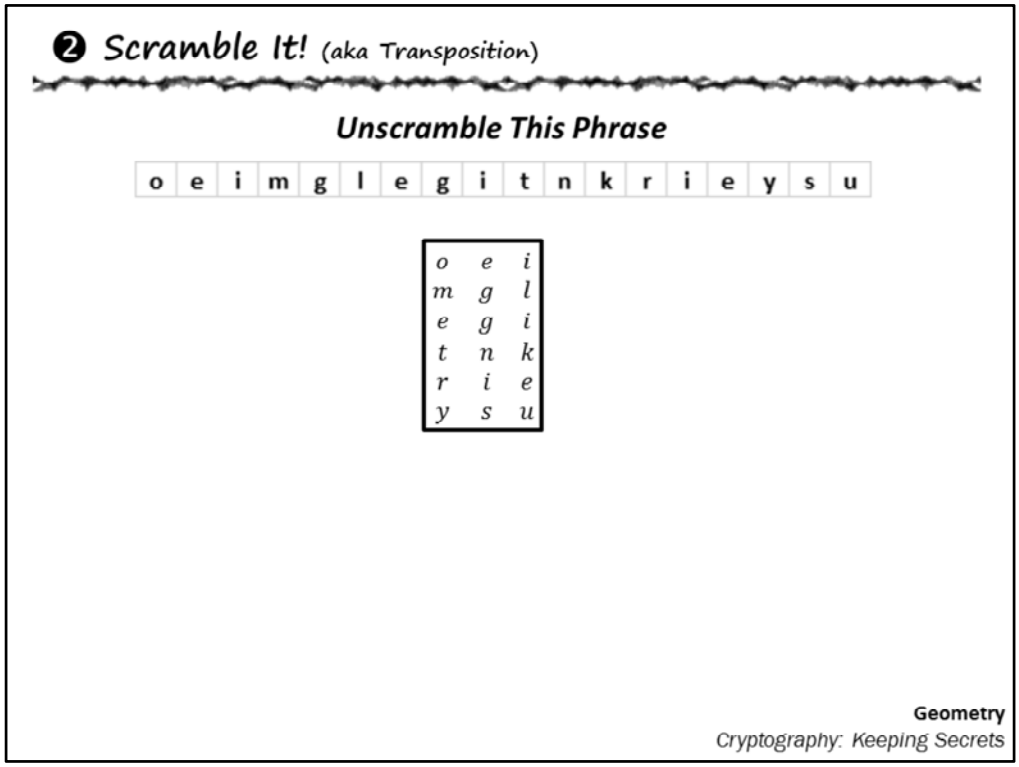
Give participants a few minutes to unscramble this.



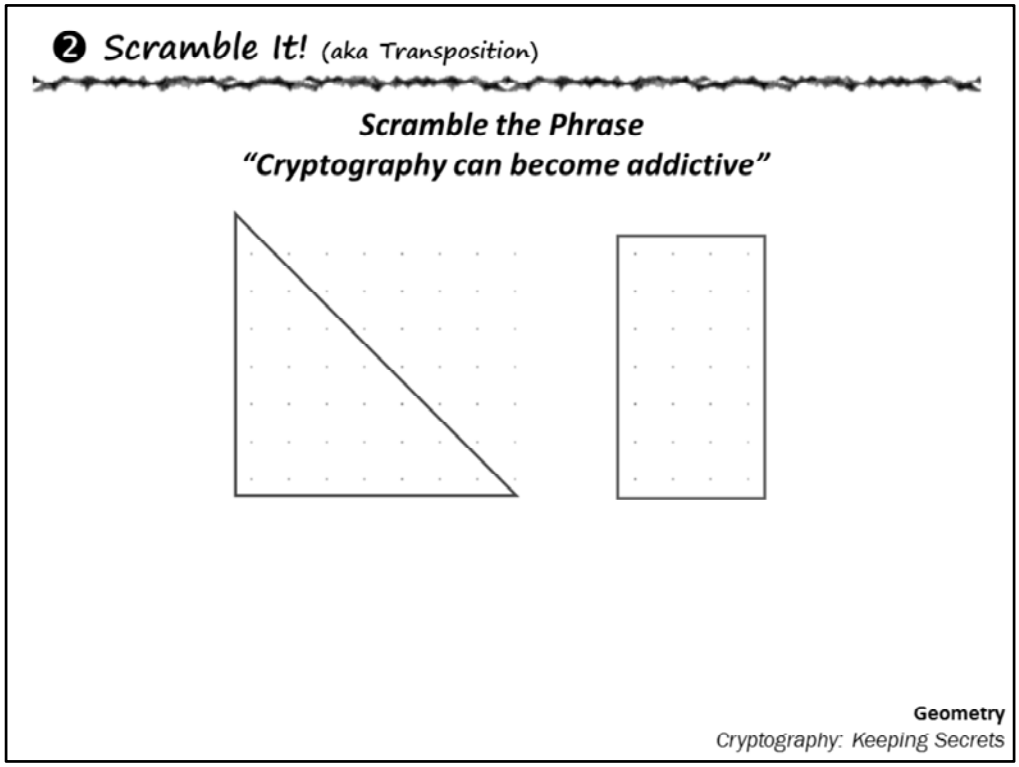
Give participants a few minutes to unscramble this.



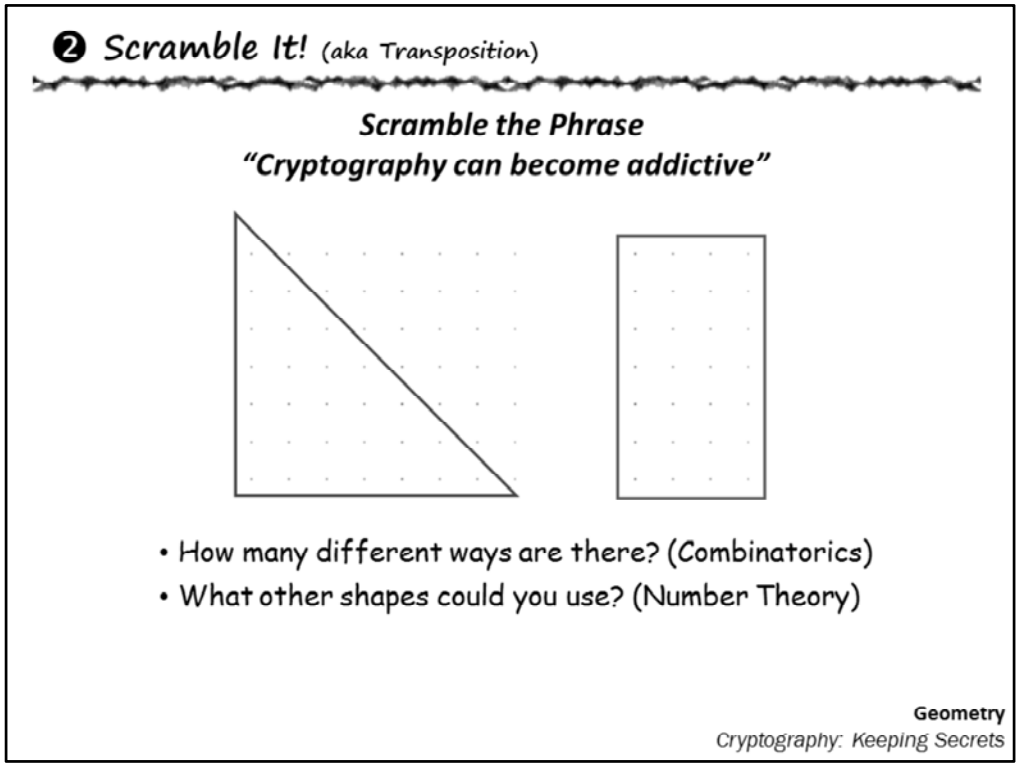
Give participants a few minutes to unscramble this.



Give participants a few minutes to unscramble this.



Give participants a few minutes to unscramble this.



Give participants a few minutes to unscramble this.

❸ Replace It! (aka Substitution)

Disguise a message by replacing characters

Define a function for converting characters to numbers

$Char$	A	B	C	D	E	F	...	Y	Z
$Position(Char)$	1	2	3	4	5	6	...	25	26

$$Domain = \{A, B, C, D, E, \dots, X, Y, Z\}$$

$$Range = \{1,2,3,4,5, \dots, 24,25,26\}$$

example: $Position(Q) = 17$

Algebra

Cryptography: Keeping Secrets

But how to make the function assignments?
Randomly define by picking numbers out of a hat example (do live?)
Advantages? Disadvantages?

❸ Replace It! (aka Substitution)

Disguise a message by replacing characters

Define a function for converting characters to numbers

$Char$	A	B	C	D	E	F	...	Y	Z
$Value(Char)$	1	2	3	4	5	6	...	25	26

$$Domain = \{A, B, C, D, E, \dots, X, Y, Z\}$$

$$Range = \{1,2,3,4,5, \dots, 24,25,26\}$$

example: $Value(Q) = 17$

- How is this similar to before? (Functions)
- How is this different than before? (Functions)

But how to make the function assignments?
Randomly define by picking numbers out of a hat example (do live?)
Advantages? Disadvantages?

❸ Replace It! (aka Substitution)

Disguise a message by replacing characters

Compose functions to replace characters with characters

$Char$	A	B	C	D	E	F	…	Y	Z
$Value(Char)$	1	2	3	4	5	6	…	25	26
$ModMixup(Value(Char))$	5	10	15	20	25	4	…	21	26
$Value^{-1}(ModMixup(Value(Char)))$	E	J	O	T	Y	D	…	U	Z

Algebra

Cryptography: Keeping Secrets

But how to make the function assignments?
Randomly define by picking numbers out of a hat example (do live?)
Advantages? Disadvantages?

i	n	v	e	r	s	e	f	u	n	c	t	i	o	n	s
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5	10	15	4	9	14	3	8	13	2	7	12	1	6	11	0
r	n	n	e	u	o	v	f	i	n	e	t	i	s	c	s

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
h	e	e	a	t	p	u	i	m	e	n	p	c	h	s	r	v	a	l	s	r	y
9	18	5	14	1	10	19	6	15	2	11	20	7	16	3	12	21	8	17	4	13	22
m	a	t	h	h	e	l	p	s	e	n	s	u	r	e	p	r	i	v	a	c	y