

Cryptography: Keeping Secrets Using Algebra and Geometry

André Mathurin

Bellarmino 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

Cryptography: Keeping Secrets Using Algebra & Geometry

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.

Cryptography: Keeping Secrets Using Algebra & Geometry

Focus on Functions
adjust as you desire.

Preliminaries

* Goals

- ✓ *Spark Ideas for Teaching Functions*
- ✓ *Articulate Fundamental Ideas of Cryptography*

* Format

- ✓ *Audience Participation + Presenter Guidance*
- ✓ *Highlight Connections/Extensions*

Cryptography: Keeping Secrets Using Algebra & Geometry

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

Preliminaries

* Goals

- ✓ *Spark Ideas for Teaching Functions*
- ✓ *Articulate Fundamental Ideas of Cryptography*

* Format

- ✓ *Audience Participation + Presenter Guidance*
- ✓ *Highlight Connections/Extensions*

* Disclaimers

- ✓ *Requires Modular Arithmetic*
- ✓ *Do Not Expect Highly Secure*

Cryptography: Keeping Secrets Using Algebra & Geometry

Modular Arithmetic basics only – will highlight extensions

Basic Elements of Cryptography – will suggest areas for more discussion

❶ **Scramble It!** (aka Transposition)

*Make the phrase "show me the math"
difficult to read by scrambling up the letters.*

Algebra
Cryptography: Keeping Secrets

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

① **Scramble It!** (aka Transposition)

**Make the phrase "show me the math"
difficult to read by scrambling up the letters.**

show me the math	VS.	showmethemath
wmet he mat hsho		wmethemathsho
wosh em eht tham		woshemehttham
weho ta mht mshe		wehotamhtmshe

- Which side is more difficult to read? (Cryptography)
- How many different scrambles are possible? (Combinatorics)
- Which of the scramble is the worst/best? (Cryptography)

Algebra

Cryptography: Keeping Secrets

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!

❶ **Scramble It!** (aka Transposition)

The Best

showmethemath

wehotamhtmshe

Random Scramble Method

Write each letter on a slip of paper, put slips in a hat, and randomly select one at a time.

- Disadvantages to this method? (Cryptography)

Algebra

Cryptography: Keeping Secrets

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.

❶ **Scramble It!** (aka Transposition)

Unscramble This Phrase

I C H A E S E T S R I S T

Algebra
Cryptography: Keeping Secrets

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

❶ *Scramble It!* (aka Transposition)

Scrambled Version

I C H A E S E T S R I S T

The Unscrambled Version

T H I S I S A S E C R E T

Algebra

Cryptography: Keeping Secrets

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

① *Scramble It!* (aka Transposition)

How do you get this

I C H A E S E T S R I S T

from this?

T H I S I S A S E C R E T

- What is the a pattern? (Cryptanalysis)

Algebra

Cryptography: Keeping Secrets

There is a pattern – it's based on Modular Arithmetic

Hint: Look for unique characters

Now that we know this patten, 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.

① 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?

① 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
$5n \pmod{13}$	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?

① *Scramble It!* (aka Transposition)

Modular Scramble Method

$Char(ModMixup(n))$

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

example: $Char(ModMixup(4)) = Char(5(4) \text{ mod } 13)$
 $= Char(20 \text{ mod } 13)$
 $= Char(7)$

$Char(ModMixup(n))$	I	C	H	A	E	S	E	T	S	R	I	S	T
-----------------------	---	---	---	---	---	---	---	---	---	---	---	---	---

Algebra

Cryptography: Keeping Secrets

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

1 Scramble It! (aka Transposition)

Modular Scramble Method

pseudo-random scramble of the phrase characters

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

$$ModMixup(n) = 5n \pmod{13}$$

Algebra

Cryptography: Keeping Secrets

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

① Scramble It! (aka Transposition)

Modular Un-Scramble Method

Use $ModMixup^{-1}(n)$

$ModMixup(n)$

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

$ModMixup^{-1}(n)$

(n)	1	2	3	4	5	6	7	8	9	10	11	12	13
$((5^{-1})n \text{ mod } 13)$	8	3	11	6	1	9	4	12	7	2	10	5	13

Algebra

Cryptography: Keeping Secrets

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

1 Scramble It! (aka Transposition)

Modular Un-Scramble Method

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

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

example: $\text{Char}(\text{ModMixup}^{-1}(4)) = \text{Char}(8(4) \bmod 13)$
 $= \text{Char}(32 \bmod 13)$
 $= \text{Char}(6)$

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

Algebra

Cryptography: Keeping Secrets

❶ Scramble It! (aka Transposition)

Modular Un-Scramble Method

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

(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

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

Algebra

Cryptography: Keeping Secrets

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

① **Scramble It!** (aka Transposition)

Scramble the phrase "inverse functions"

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

Algebra
Cryptography: Keeping Secrets

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

① **Scramble It!** (aka Transposition)

Scramble the phrase "inverse functions"

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

Algebra

Cryptography: Keeping Secrets

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

① *Scramble It!* (aka Transposition)

Unscramble the phrase

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

Algebra

Cryptography: Keeping Secrets

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

① **Scramble It!** (aka Transposition)

Unscramble the phrase

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

Algebra

Cryptography: Keeping Secrets

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

② **Scramble It!** (aka Transposition)

Unscramble This Phrase

c	a	e	m	f	d	o	u	n	d	e
---	---	---	---	---	---	---	---	---	---	---

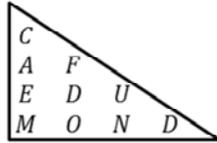
Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

② **Scramble It!** (aka Transposition)

Unscramble This Phrase

c a e m f d o u n d e



Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

② **Scramble It!** (aka Transposition)

Unscramble This Phrase

o e i m g l e g i t n k r i e y s u

Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

② **Scramble It!** (aka Transposition)

Unscramble This Phrase

o e i m g l e g i t n k r i e y s u

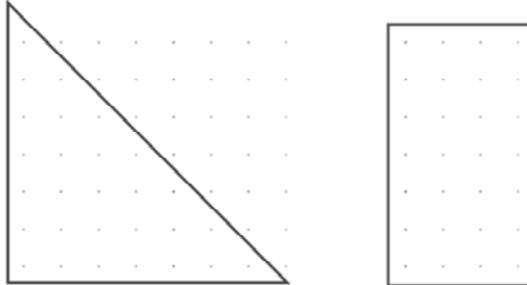
o	e	i
m	g	l
e	g	i
t	n	k
r	i	e
y	s	u

Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

② **Scramble It!** (aka Transposition)

Scramble the Phrase
"Cryptography can become addictive"

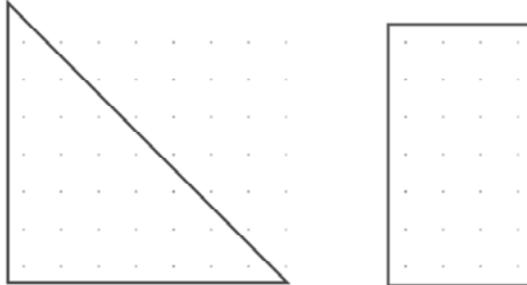


Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

② **Scramble It!** (aka Transposition)

Scramble the Phrase
"Cryptography can become addictive"



- How many different ways are there? (Combinatorics)
- What other shapes could you use? (Number Theory)

Geometry
Cryptography: Keeping Secrets

Give participants a few minutes to unscramble this.

③ *Replace It!* (aka *Substitution*)

Disguise a message by replacing characters

Define a function for converting characters to numbers

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

Domain = {A, B, C, D, E, ..., X, Y, Z}

Range = {1, 2, 3, 4, 5, ..., 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?

③ *Replace It!* (aka *Substitution*)

Disguise a message by replacing characters

Define a function for converting characters to numbers

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

Domain = {A, B, C, D, E, ..., X, Y, Z}

Range = {1, 2, 3, 4, 5, ..., 24, 25, 26}

example: $Value(Q) = 17$

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

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?

③ *Replace It!* (aka *Substitution*)

Disguise a message by replacing characters

Compose functions to replace characters with characters

<i>Char</i>	A	B	C	D	E	F	...	Y	Z
<i>Value(Char)</i>	1	2	3	4	5	6	...	25	26
<i>ModMixup(Value(Char))</i>	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