Cryptography: Keeping Secrets Using Algebra and Geometry

André Mathurin
Bellarmine College Preparatory (San Jose, CA)

With increasing reliance on email and texting, how can mathematics help ensure that these remain private? Learn ways and get ideas for engaging students in the basic ideas of cryptography in the context of teaching algebra and geometry.

e	g	i	a	l		d	c	h	n	s		w	l	n	t	t		o	a	i	a	i		f	l	e	k	d

BC Association of Math Teachers

SCALING NEW HEIGHTS

What to Expect

- Goals
  - ✓ *Spark Ideas for Teaching Algebra & Geometry*
  - ✓ *Introduce Transposition Ciphers*
- Mathematics
  - ✓ *Functions (evaluate, domain & range, inverses)*
  - ✓ *Modular Arithmetic (equivalence classes, inverses)*

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.

Scramble It!

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

Scramble It!

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

show	me	the	math
wmet	he	mat	hsho
wosh	em	eht	tham
weho	ta	mht	mshe

vs.

showmethemath
wmethemathsho
woshemehttham
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)

Scramble It!

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)

Non-Random Scrambles

Unscramble This Phrase

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

Non-Random Scrambles

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

Non-Random Scrambles

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)

Non-Random Scrambles

Position Function

$char(n)$ = the n^{th} character of the text

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: $char(9) = E$

Non-Random Scrambles

Mod-Based Scrambling Function

$$scram(n) = kn \ (mod \ \ m)$$

where m *is the length of the text,* k *is an integer relatively prime to* m*, and* n *is a positive integer less than or equal to* m

$$k = 5 \ and \ m = 13$$

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

$= 45 \ (mod \ 13)$

$= 13 + 13 + 13 + 6 \ (mod \ 13)$

$= 6 \ (mod \ 13)$

Non-Random Scrambles

Enciphering Function

$char(scram(n))$ = the character to place in the nth position

example: $char(scram(4)) = char\ (5 \cdot 4\ (mod\ 13))$
$= char\ (20\ (mod\ 13))$
$= char\ (7)$
$= A$

$k = 5\ and\ m = 13$

$Char(n)$	T	H	I	S	I	S	A	S	E	C	R	E	T
n	1	2	3	4	5	6	7	8	9	10	11	12	13
$scram(n)$	5	10	2	7	12	4	9	1	6	11	3	8	0
$char(scram(n))$	I	C	H	A	E	S	E	T	S	R	I	S	T

Non-Random Scrambles

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

Non-Random Scrambles

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

Un-Scramble It

How do you reverse the effects of the scam function?

Obviously, just apply the function $scram^{-1}$
which should be divide by k right?

Un-Scramble It

How do you reverse the effects of the scam function?

Obviously, just apply the function $scram^{-1}$
which should be divide by k right?

$$k = 5 \; and \; m = 13$$

example: $scram^{-1}(8) = 8 \div 5 (mod\ 13)$
$= 1.6\ (mod\ 13)$
$= Yikes!$

Defining the $scram^{-1}$ function as division yields some values that are not part of the domain ☹

Can you reverse the effects of the scam function?
Yes.

Un-Scramble It!

Isn't division just a shortcut for multiplication?

$$4 \cdot 5 \cdot ?? = 4 \ (mod\ 13)$$

$$?? = \frac{1}{5} = 5^{-1}$$

$$5 \cdot ?? = 1 \ (mod\ 13)$$

Un-Scramble It

Isn't division just a shortcut for multiplication?

$$4 \cdot 5 \cdot ?? = 4 \ (mod\ 13)$$

$$?? = \frac{1}{5} = 5^{-1}$$

$$5 \cdot ?? = 1 \ (mod\ 13)$$

T	H	I	S	I	S	A	C	E	C	R	E	T
1	2	3	4	5	6	7	8	9	10	11	12	13
5	10	2	7	12	4	9	1	6	11	3	8	0
I	C	H	A	E	S	E	I	S	R	I	S	T

Algebra

Cryptography: Keeping Secrets

Un-Scramble It

Deciphering Function

$char\left(scram^{-1}(n)\right)$ = the character to place in the nth position

example: $char\left(scram^{-1}(6)\right) = char\,(\,8 \cdot 6 \ (mod\ 13)\,)$

$= char\,(\,48\ (mod\ 13)\,)$

$= char\,(\,13 + 13 + 13 + 9\ (mod\ 13)\,)$

$= char\,(\,9\,) =$ S

$k = 5\ and\ m = 13$

$Char(n)$	I	C	H	A	E	S	E	T	S	R	I	S	T
n	1	2	3	4	5	6	7	8	9	10	11	12	13
$scram(n)$	8	3	11	6	1	9	4	12	7	2	10	5	0
$char\left(scram^{-1}(n)\right)$	T	H	I	S	I	S	A	S	E	C	R	E	T

Un-Scramble It

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

Un-Scramble It

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

Non-Random Scrambles

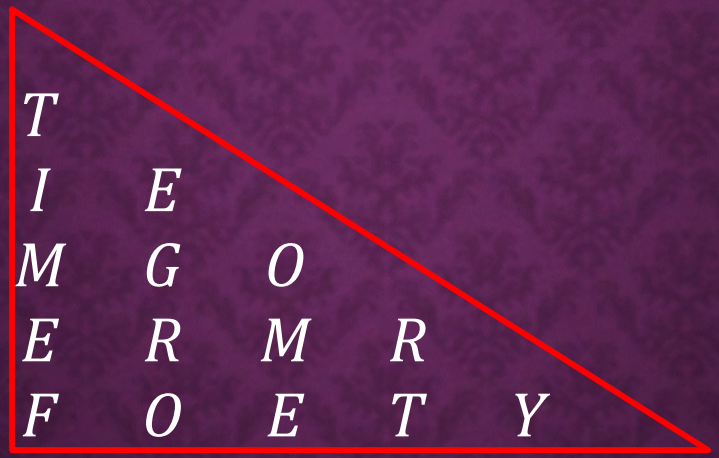
Unscramble This Phrase

t	i	e	m	g	o	r	r	m	r	f	o	e	t	y

Non-Random Scrambles

Unscramble This Phrase

t	i	e	m	g	o	e	r	m	r	f	o	e	t	y



Un-Scramble It!

Unscramble This Phrase

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

Un-Scramble It!

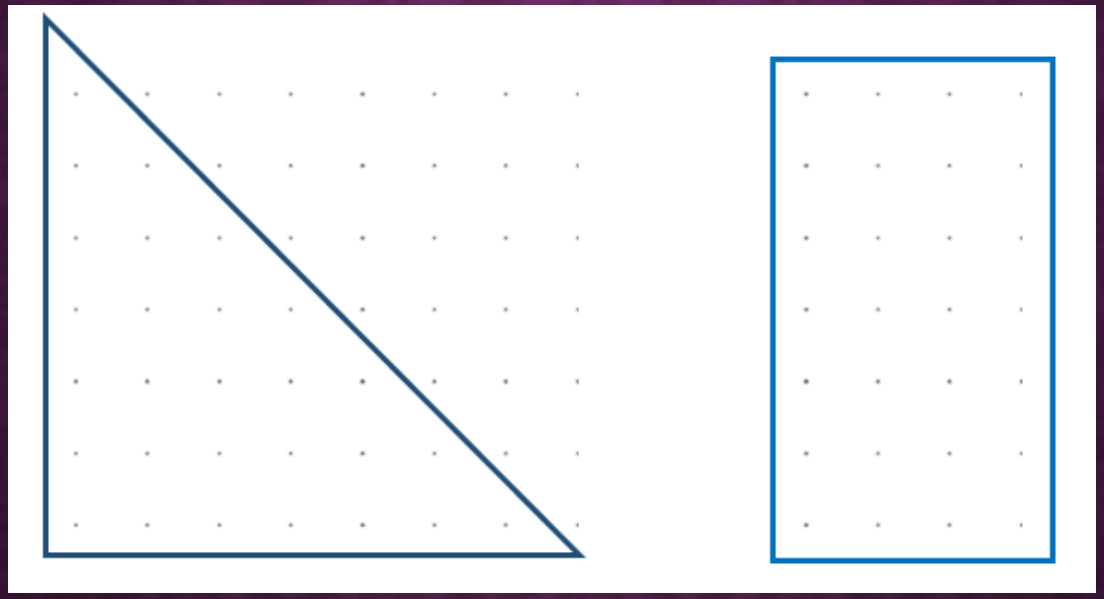
Unscramble This Phrase

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

Non-Random Scrambles

Scramble the Phrase
"Cryptography can become addictive"



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

e	g	i	a	l		d	c	h	n	s		w	l	n	t	t		o	a	i	a	i		f	l	e	k	d

e	g	i	a	l
d	c	h	n	s
w	l	n	t	t
o	a	i	a	i
f	l	e	k	d

- **Contact & Resource Information**

amathurin@bcp.org

http://tinyurl.com/amathurinNWMC

BC Association of Math Teachers

SCALING NEW HEIGHTS