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

Preliminaries

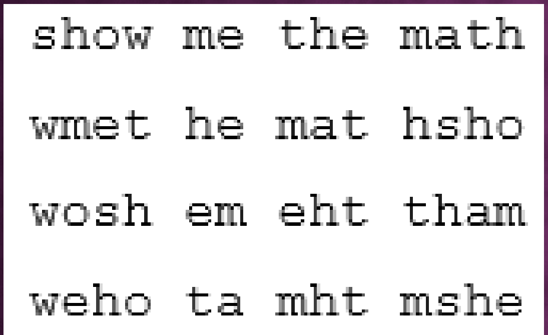
- ✷ Goals
  - ✓ *Spark Ideas for Teaching Functions*
  - ✓ *Introduce Cryptography using Algebra & Geometry*
- ✷ Format
  - ✓ *Audience Participation + Presenter Guidance*
  - ✓ *Highlight Connections/Extensions*
- ✷ Disclaimers
  - ✓ *Requires Modular Arithmetic*
  - ✓ *Do Not Expect Highly Secure*

➊ Scramble It! (aka Transposition)

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

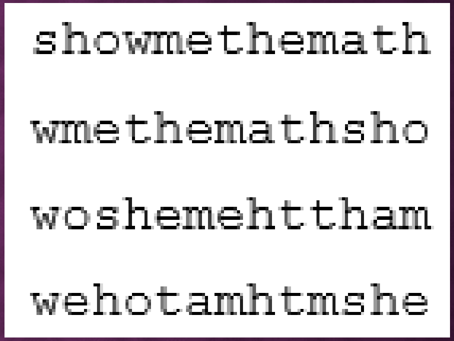
➊ Scramble It! (aka Transposition)

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.

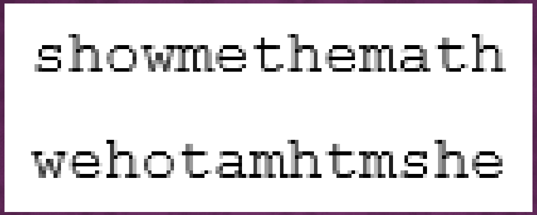


```
showmethemath
wmethemathsho
woshemehttham
wehotamhtmshe
```

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

➊ 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)

❶ Scramble It! (aka Transposition)

Unscramble This Phrase

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

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

❶ 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)

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: $\boldsymbol{Char(9) = E}$

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

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

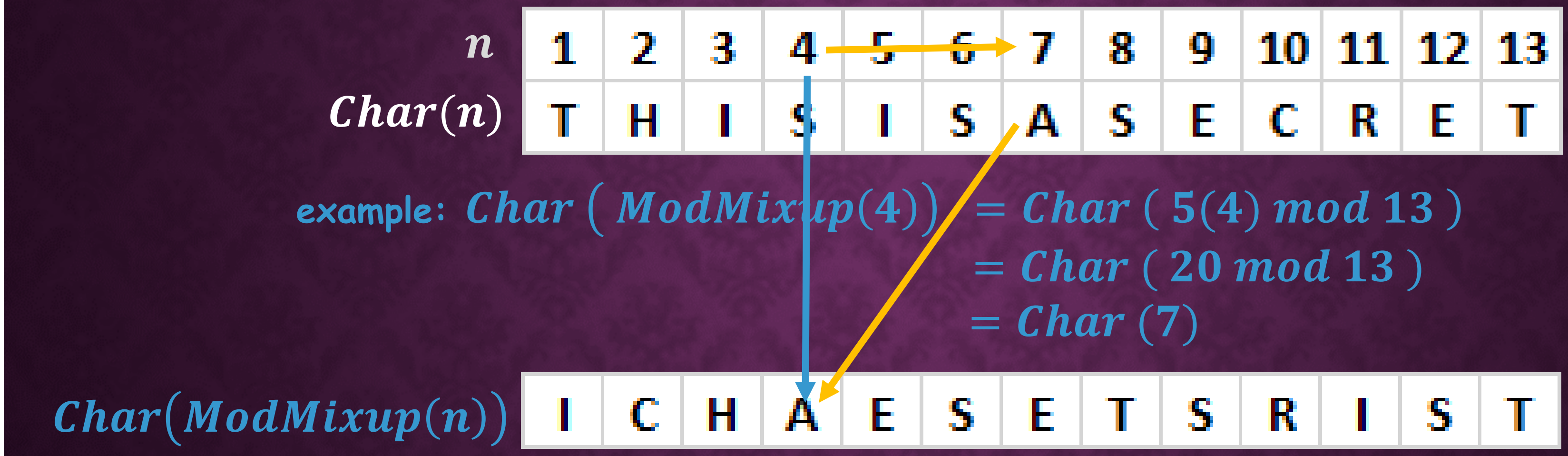
$$Range = \{1,2,3,4,5,6,7,8,9,10,11,12,13\}$$

example: $ModMixup(5) = 12$

❶ Scramble It! (aka Transposition)

Modular Scramble Method

$$Char\big(ModMixup(n)\big)$$



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

example: $Char\,\big(\,ModMixup(4)\big) = Char\,(\,5(4)\ mod\ 13\,)$

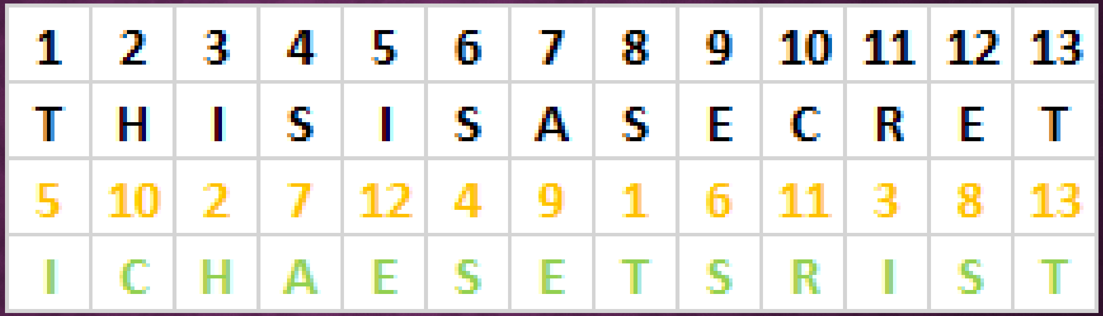
$= Char\,(\,20\ mod\ 13\,)$

$= Char\,(7)$

❶ Scramble It! (aka Transposition)

Modular Scramble Method

pseudo-random scramble of the phrase characters

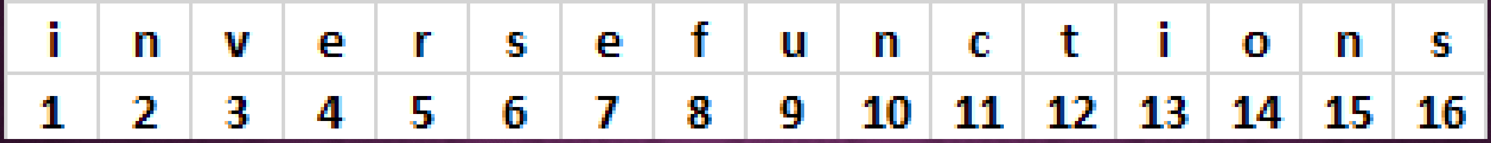


n	1	2	3	4	5	6	7	8	9	10	11	12	13
$Char(n)$	T	H	I	S	I	S	A	S	E	C	R	E	T
$ModMixup(n)$	5	10	2	7	12	4	9	1	6	11	3	8	13
$Char\big(ModMixup(n)\big)$	I	C	H	A	E	S	E	T	S	R	I	S	T

$$ModMixup\ (n) = 5n\ (mod\ 13)$$

❶ Scramble It! (aka Transposition)

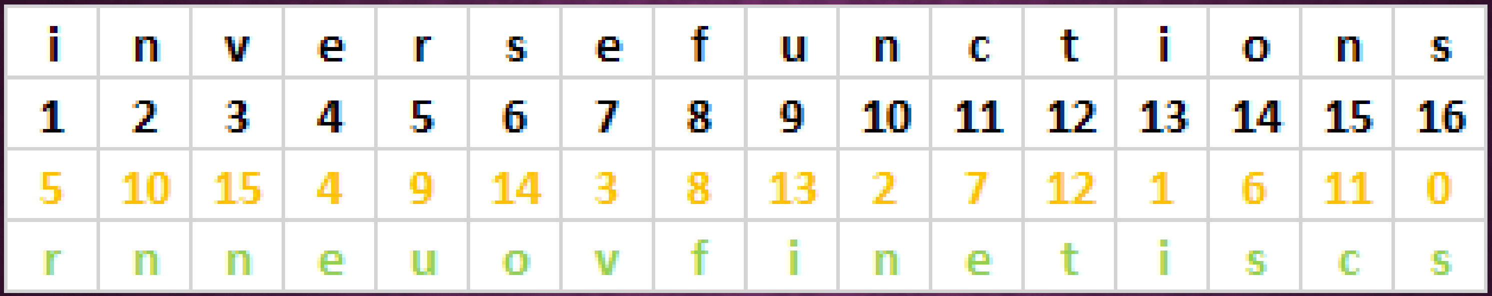
Scramble the phrase "inverse functions"



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

➊ 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

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

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

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

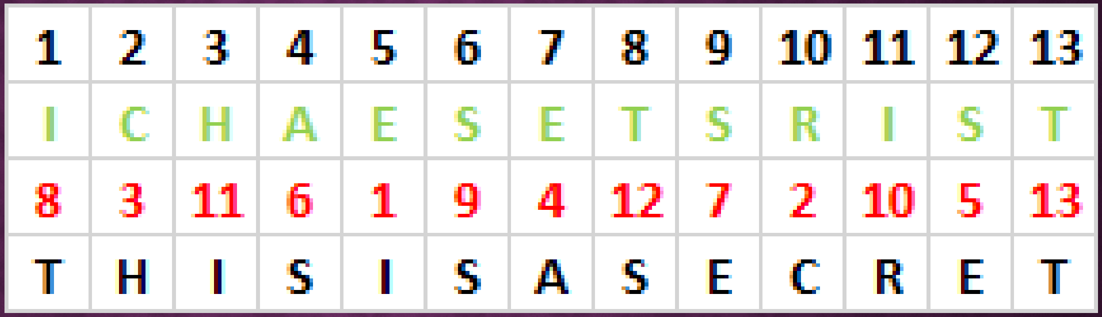
$= Char\,(\,32\;mod\;13\,)$

$= Char\,(6)$

➊ Scramble It! (aka Transposition)

Modular *Un*-Scramble Method

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

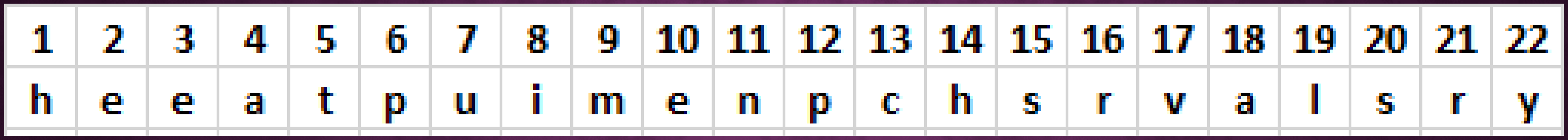


(n)	1	2	3	4	5	6	7	8	9	10	11	12	13
$Char\ (n)$	I	C	H	A	E	S	E	T	S	R	I	S	T
$ModMixup^{-1}\ (n)$	8	3	11	6	1	9	4	12	7	2	10	5	13
$Char\ (\ ModMixup^{-1}\ (n)\ )$	T	H	I	S	I	S	A	S	E	C	R	E	T

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

❶ Scramble It! (aka Transposition)

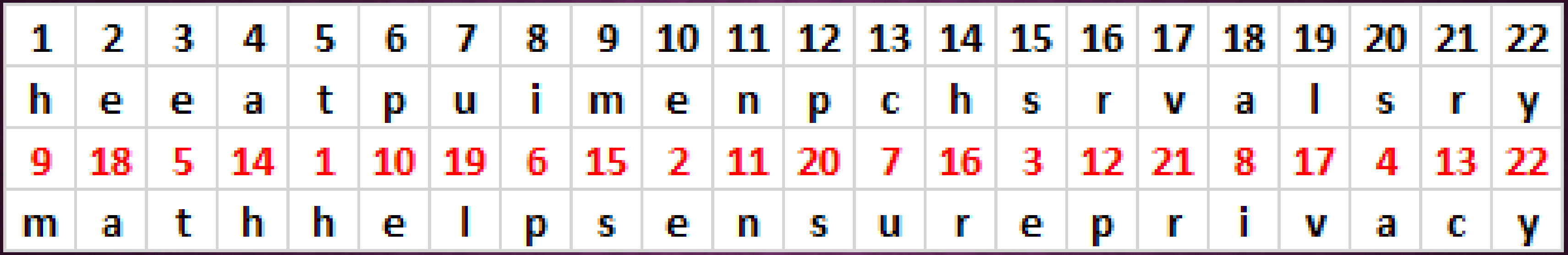
Unscramble the phrase



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

❶ 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

❷ Scramble It! (aka Transposition)

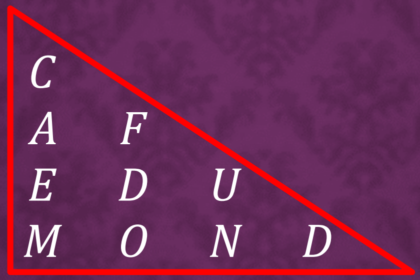
Unscramble This Phrase

c	a	e	m	f	d	o	u	n	d	e

❷ Scramble It! (aka Transposition)

Unscramble This Phrase

c	a	e	m	f	d	o	u	n	d	e



C

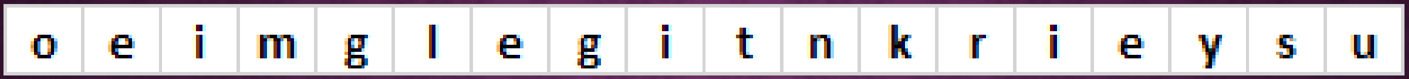
A F

E D U

M O N D

❷ 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

❷ Scramble It! (aka Transposition)

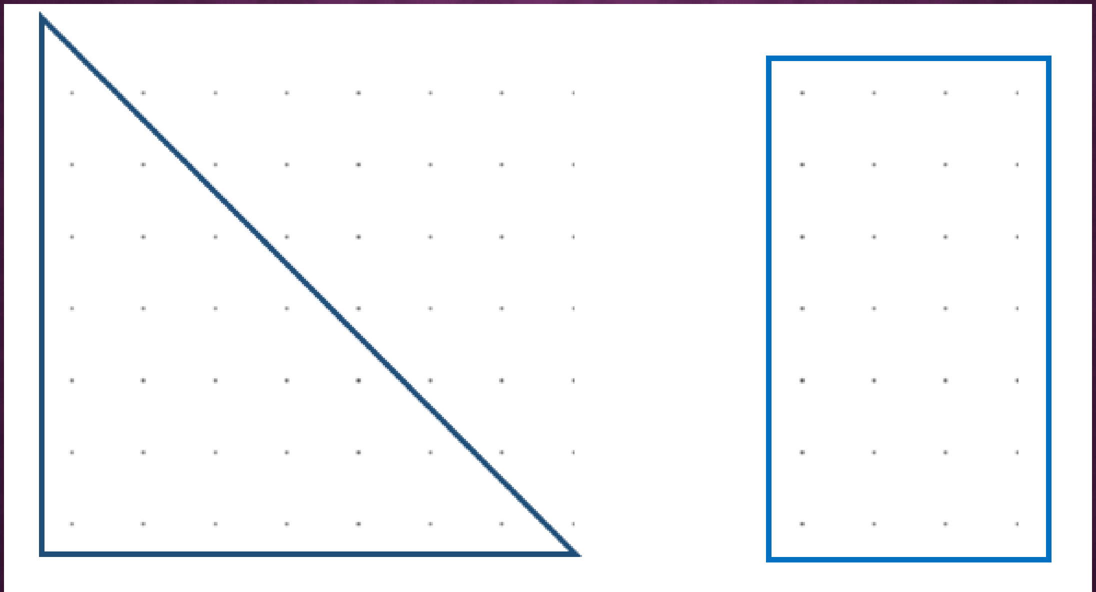
Unscramble This Phrase

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*

❷ Scramble It! (aka Transposition)

Scramble the Phrase
"Cryptography can become addictive"

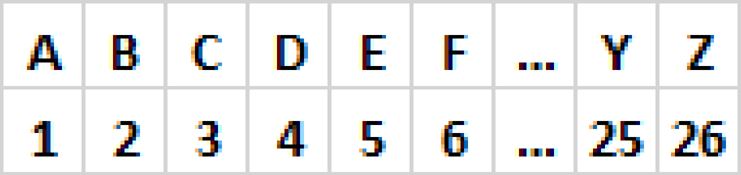


- How many different ways are there? (Combinatorics)
- What other shapes could you use? (Number Theory)

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

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

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

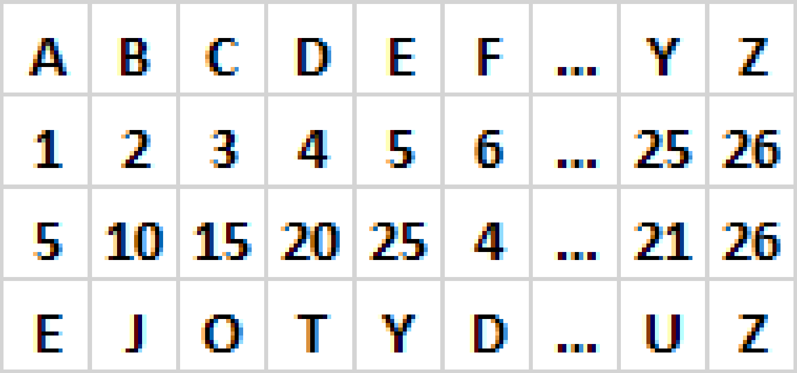
example: $\boldsymbol{Value(Q) = 17}$

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

❸ Replace It! (aka Substitution)

Disguise a message by replacing characters

Compose functions to replace characters with characters

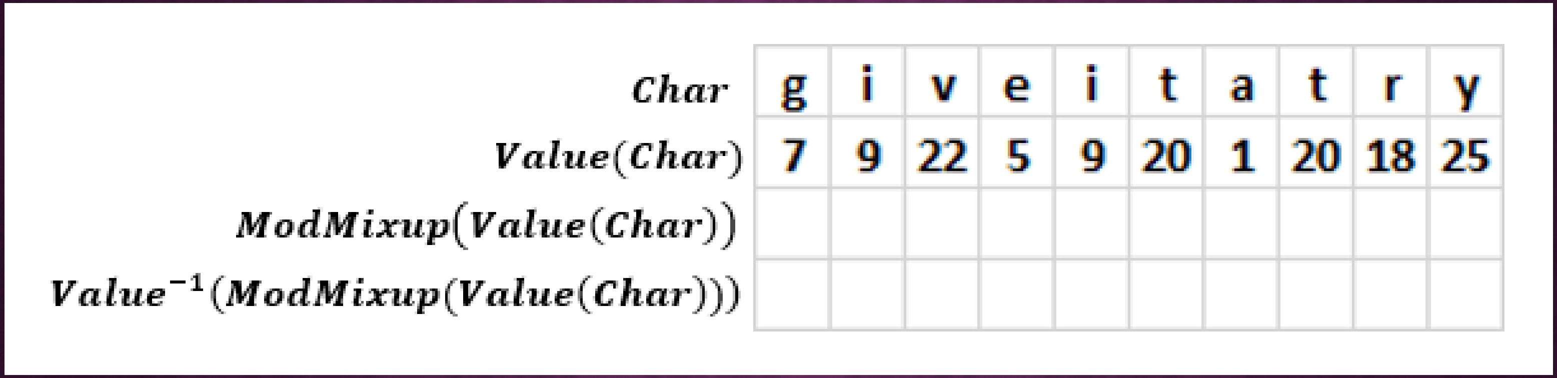


$Char$	A	B	C	D	E	F	...	Y	Z
$Value(Char)$	1	2	3	4	5	6	...	25	26
$ModMixup(Value(Char))$	5	10	15	20	25	4	...	21	26
$Value^{-1}\left(ModMixup(Value(Char))\right)$	E	J	O	T	Y	D	...	U	Z

❸ Replace It! (aka Substitution)

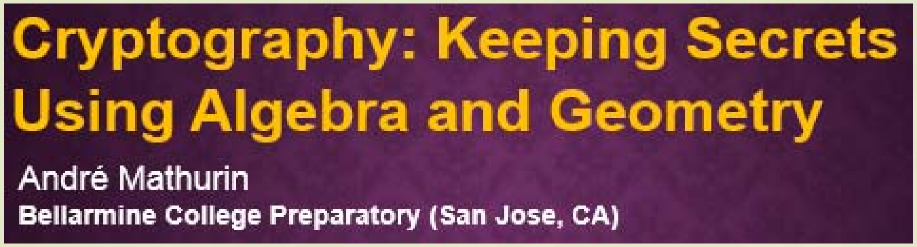
Disguise a message by replacing characters

Compose functions to replace characters with characters



$Char$	g	i	v	e	i	t	a	t	r	y
$Value(Char)$	7	9	22	5	9	20	1	20	18	25
$ModMixup(Value(Char))$										
$Value^{-1}(ModMixup(Value(Char)))$										

2014 NCTM ANNUAL MEETING & EXPOSITION
April 9–12 • New Orleans


Cryptography: Keeping Secrets Using Algebra and Geometry

André Mathurin
Bellarmine College Preparatory (San Jose, CA)

Rate this presentation on the conference app! **www.nctm.org/confapp**

Download available presentation handouts from the Online Planner! **www.nctm.org/planner**

Join the conversation! Tweet us using the hashtag **#NCTMNOLA**

NCTM
NATIONAL COUNCIL OF
TEACHERS OF MATHEMATICS