Teaching Inverse Functions with Cryptography

An Interactive Approach

Lisa Harden[1] Leandro Junes[2]

[1]St. Louis CC - Meramec
Kirkwood, MO.
lharden6@stlcc.edu

[2]University of South Carolina-Sumter
Sumter, SC.
junesl@uscsumter.edu

2011 AMATYC Conference
November 11

Codes in Ancient Roman Battle

- If Julius Caesar wished to call his troops home, he may have sent a message such as
  - -Uhwxuq wr Urph.
- Can be deciphered if person knows the key.
- Secrecy maintained if a person does not know the key. Picture taken from [2].

Codes in Ancient Roman Battle

- To obtain the encoded message "Uhwxuq wr Urph" each letter of the original message was simply replaced with the letter three places to the right.
  - "Caesar Cipher"

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M
Encoded:	D	E	F	G	H	I	J	K	L	M	N	O	P

Original:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encoded:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Codes in Ancient Roman Battle

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M
Encoded:	D	E	F	G	H	I	J	K	L	M	N	O	P

Original:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encoded:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- "Uhwxuq wr Urph" decodes to "Return to Rome"

Picture taken from [2]

How does this relate to functions?

- Instead of thinking "Shift each letter 3 places to the right" we can think of functions with input and output.

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	29	21	22	23	23	25

  - Input: a number that represents a letter.
  - Output: the number plus 3.
    - Input: x.
    - Output: $x+3$
      $f(x) = x+3$

Ciphers

- A cipher is a method for creating secret messages.
- The purpose of using a cipher is to exchange information securely.

Associate each Letter to a Number

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

t	u	v	w	x	y	z	A	B	C	D	E	F	G	H	I	J
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	?
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Each Integer Correspond to a Letter

- If n is any integer, then the remainder r of $n \div 53$ is a number in $\{0, 1, \ldots, 52\}$.
- This correspondence is not injective.

Each Integer Correspond to a Letter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

t	u	v	w	x	y	z	A	B	C	D	E	F	G	H	I	J
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	?
36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Each Integer Modulo 53 Corresponds to a Letter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$

t	u	v	w	x	y	z	A	B	C	D	E	F	G	H	I	J
$\overline{19}$	$\overline{20}$	$\overline{21}$	$\overline{22}$	$\overline{23}$	$\overline{24}$	$\overline{25}$	$\overline{26}$	$\overline{27}$	$\overline{28}$	$\overline{29}$	$\overline{30}$	$\overline{31}$	$\overline{32}$	$\overline{33}$	$\overline{34}$	$\overline{35}$

K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	?
$\overline{36}$	$\overline{37}$	$\overline{38}$	$\overline{39}$	$\overline{40}$	$\overline{41}$	$\overline{42}$	$\overline{43}$	$\overline{44}$	$\overline{45}$	$\overline{46}$	$\overline{47}$	$\overline{48}$	$\overline{49}$	$\overline{50}$	$\overline{51}$	$\overline{52}$

All non-zero Integers Modulo 53 have Multiplicative Inverses

Examples

- Since $25 \times 17 = 425$ and $425 \div 53$ leaves remainder 1, $\frac{1}{25} = 17$.
- Since $4 \times 40 = 160$ and $160 \div 53$ leaves remainder 1, $\frac{1}{4} = 40$.

Theorem

If p is a prime number, then every non-zero integer module p has a multiplicative inverse.[a]

[a] For a proof see [1, Fraleigh]

All Integers Modulo 53 have "Exact" Cubic Roots

Definition

We say that $\sqrt[3]{x} = y$, if $y^3 = x$.

Examples

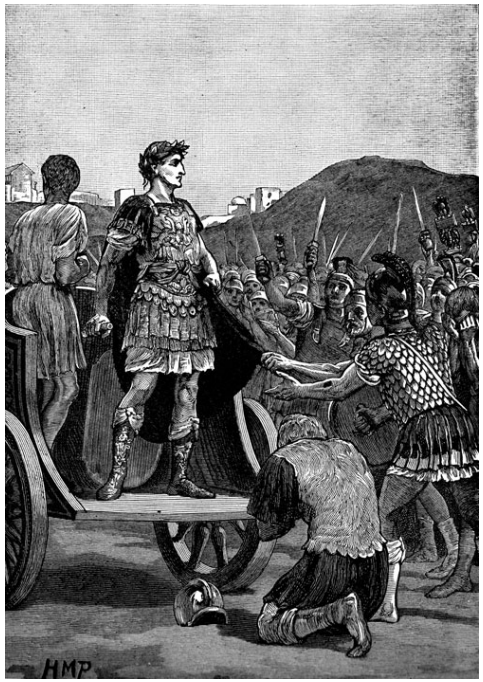
- Since $1^3 = 1$, $\sqrt[3]{1} = 1$.
- Since $18^3 = 5832$ and $5832 \div 53$ leaves remainder 2, $\sqrt[3]{2} = 18$.

Theorem

If p is a prime number of the form $3k+2$, then every integer module p has a unique cubic root. That is, $\sqrt[3]{x}$ is a unique integer module p.

An Example

In 47 BC, Julius Caesar conquered Pharnaces II of Pontus in the city of Zela in present day Turkey. He claimed to have done so in 4 hours. Caesar decides to send an encrypted message back to the Senate in Rome.

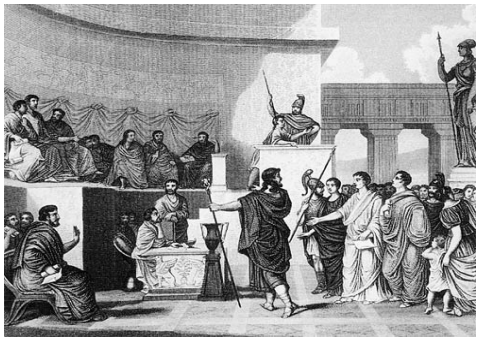


An Example

Before Caesar leaves, they decide to use the linear function $f(x) = 3x + 1$ to encrypt/decrypt all comunications.

Caesar

Senate



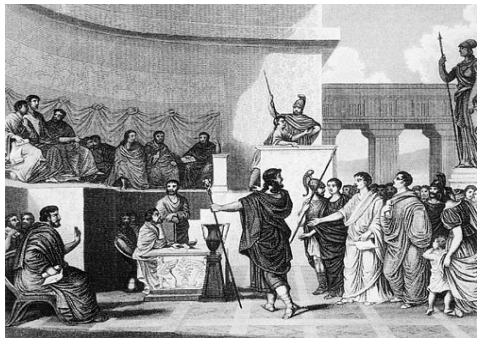
$$f(x) = 3x + 1$$

An Example

Caesar is now gone.

Caesar

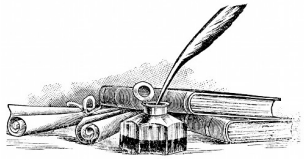
Senate



An Example

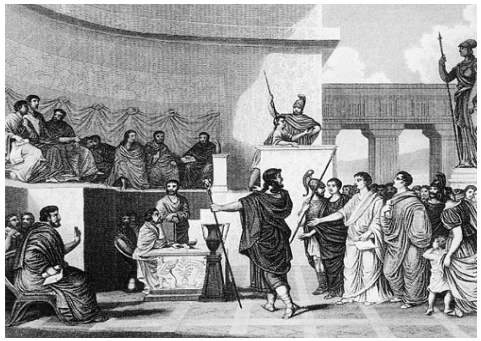
Caesar wants to send the Senate a message.

Caesar

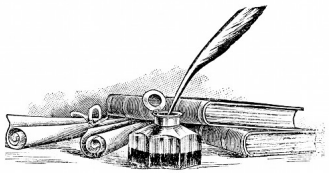


Veni, vidi, vici

Senate



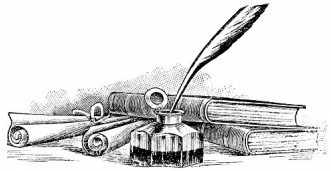
An Example



$f(x) = 3x + 1$ Veni, vidi, vici

Text	V	e	n	i		v	i	d	i		v	i	c	i
x	47	4	13	8		21	8	3	8		21	8	2	8

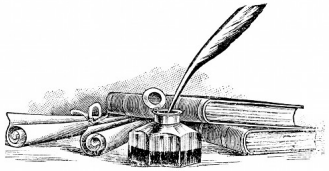
An Example



$f(x) = 3x + 1$ Veni, vidi, vici

Text	V	e	n	i		v	i	d	i		v	i	c	i
x	47	4	13	8		21	8	3	8		21	8	2	8
$f(x) = 3x + 1$	142	13	40	25		64	25	10	25		64	25	7	25

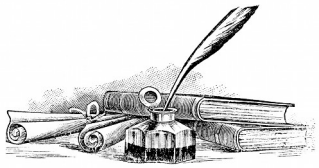
An Example



$f(x) = 3x + 1$ Veni, vidi, vici

Text	V	e	n	i		v	i	d	i		v	i	c	i
x	47	4	13	8		21	8	3	8		21	8	2	8
$f(x) = 3x + 1$	142	13	40	25		64	25	10	25		64	25	7	25
Modulo 53	36	13	40	25		11	25	10	25		11	25	7	25

An Example

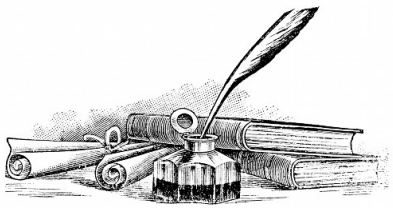


$f(x) = 3x + 1$ Veni, vidi, vici

Text	V	e	n	i		v	i	d	i		v	i	c	i
x	47	4	13	8		21	8	3	8		21	8	2	8
$f(x) = 3x + 1$	142	13	40	25		64	25	10	25		64	25	7	25
Modulo 53	36	13	40	25		11	25	10	25		11	25	7	25
Cipher Text	K	n	O	z		l	z	k	z		l	z	h	z

An Example

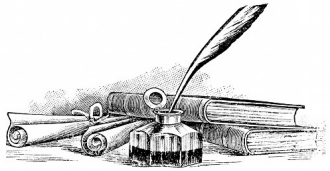
Caesar



Veni, vidi, vici
KnOz, Izkz, Izhz

An Example

Caesar

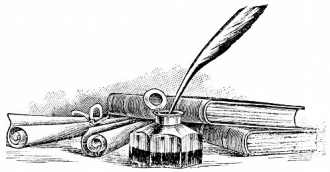


KnOz, lzkz, lzhz

Senate

An Example

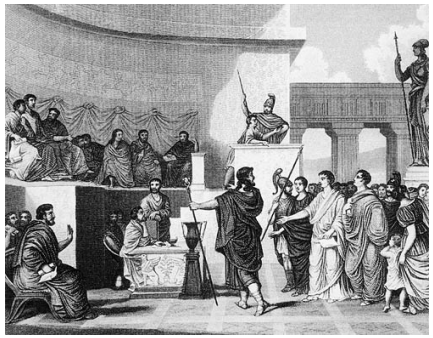
Caesar



KnOz, Izkz, Izhz $\longrightarrow$

Enemy

Senate

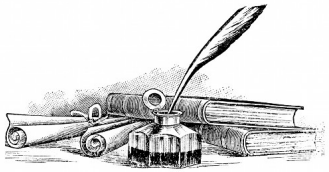


An Example

Caesar

Enemy

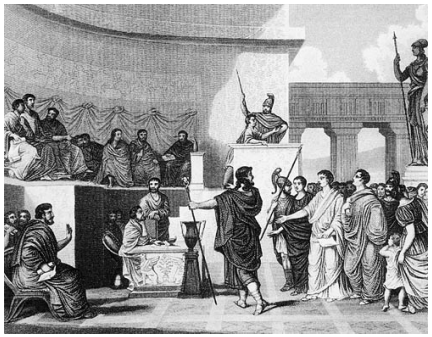
Senate

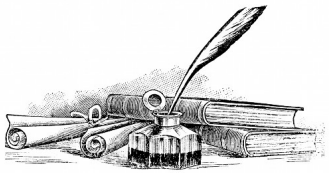


KnOz, Izkz, Izhz

An Example

Senate



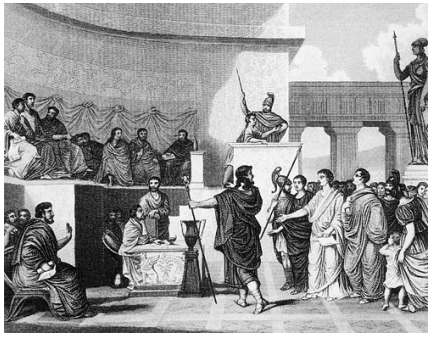


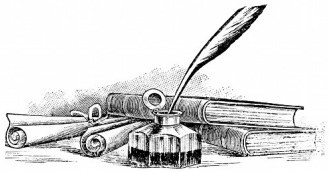
$f(x) = 3x + 1$ KnOz, lzkz, lzhz

Cipher Text	K	n	O	z		l	z	k	z		l	z	h	z
x	36	13	40	25		11	25	10	25		11	25	7	25

An Example

Senate





$$f^{-1}(x) = \frac{1}{3}x - \frac{1}{3}$$

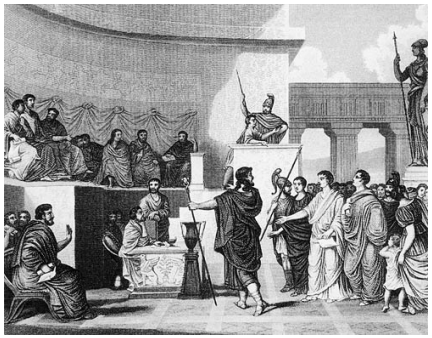
KnOz, lzkz, lzhz

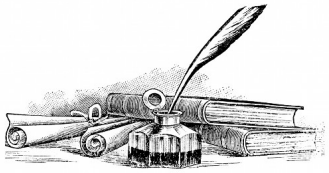
Cipher Text	K	n	O	z		l	z	k	z		l	z	h	z
x	36	13	40	25		11	25	10	25		11	25	7	25

An Example

We know that $\frac{1}{3} = 18$ modulo 53 because $18 \times 3 = 54$ that leaves residue 1 when divided by 53. Thus,

Senate



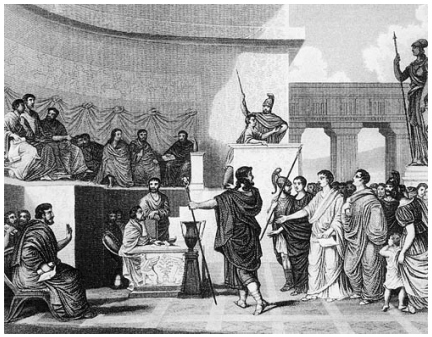


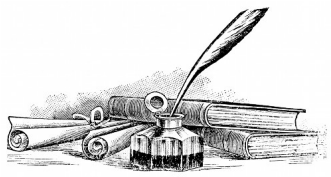
$f^{-1}(x) = 18x - 18$ KnOz, lzkz, lzhz

Cipher Text	K	n	O	z		l	z	k	z		l	z	h	z
x	36	13	40	25		11	25	10	25		11	25	7	25

An Example

Senate



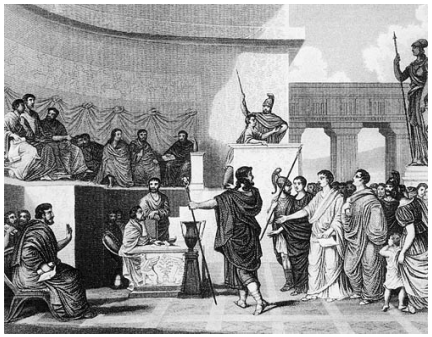


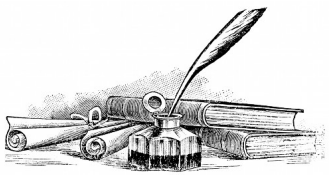
$f^{-1}(x) = 18x - 18$ KnOz, lzkz, lzhz

Cipher Text	K	n	O	z	l	z	k	z	l	z	h	z
x	36	13	40	25	11	25	10	25	11	25	7	25
$f^{-1}(x) = 18x - 18$	630	216	702	432	180	432	162	432	180	432	108	432

An Example

Senate



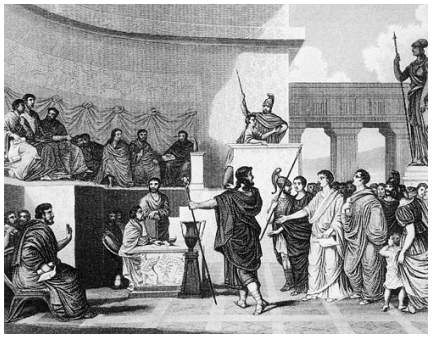


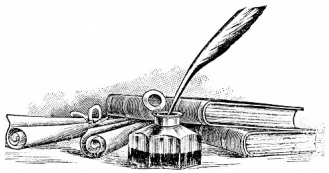
$f^{-1}(x) = 18x - 18$ KnOz, lzkz, lzhz

Cipher Text	K	n	O	z	l	z	k	z	l	z	h	z
x	36	13	40	25	11	25	10	25	11	25	7	25
$f^{-1}(x) = 18x - 18$	630	216	702	432	180	432	162	432	180	432	108	432
Module 53	47	4	13	8	21	8	3	8	21	8	2	8

An Example

Senate





$f^{-1}(x) = 18x - 18$ KnOz, lzkz, lzhz

Cipher Text	K	n	O	z	l	z	k	z	l	z	h	z
x	36	13	40	25	11	25	10	25	11	25	7	25
$f^{-1}(x) = 18x - 18$	630	216	702	432	180	432	162	432	180	432	108	432
Module 53	47	4	13	8	21	8	3	8	21	8	2	8
Text	V	e	n	i	v	i	d	i	v	i	c	i

isn't this too much for students to do?

- Our software simplifies the process by handling all minor detail computations (software computes everything modulo 53).
- Students only need to know how to compute the inverse of a function. They do NOT need to know arithmetic modulo 53.

isn't this too much for students to do?

- Our software simplifies the process by handling all minor detail computations (software computes everything modulo 53).
- Students only need to know how to compute the inverse of a function. They do NOT need to know arithmetic modulo 53.

Preview of the software

Function Name	Algebraic Form	Restrictions
Linear Function	$f(x) = \frac{a}{b}x + \frac{c}{d}$	a, b and d cannot be multiples of 53.
Rational Function	$f(x) = \frac{ax+b}{53cx+d}$	a and d cannot be multiples of 53.
Cubic Function	$f(x) = \frac{a}{b}x^3 + \frac{c}{d}$	a, b and d cannot be multiples of 53.
Cubic Root Function	$f(x) = \sqrt[3]{\frac{a}{b}x + \frac{c}{d}}$	a, b and d cannot be multiples of 53.

All numbers a, b, c and d must be integers in the interval $[-2147483648, 2147483647]$

Preview of the software

```
Enter the message you want to encrypt/decrypt: Veni, vidi, vici

Enter 1 for linear.
Enter 2 for rational.
Enter 3 for cubic.
Enter 4 for cubic root.

Enter your choice:
```

Preview of the software

```
Enter 1 for linear.
Enter 2 for rational.
Enter 3 for cubic.
Enter 4 for cubic root.

Enter your choice: 1

Remember that a Linear Function has the form
                        a        c
              f(x) = --- x + ---
                        b        d

Enter the integer a: |
```

Preview of the software

The function f is given by $f(x) = 3x + 1 = \frac{3}{1}x + \frac{1}{1}$

```
Enter the integer a: 3
Enter the integer b: 1

Enter the integer c: 1
Enter the integer d: 1

The new message is: KnOz, lzkz, lzhz


Do you want to continue [Pres `y` for yes] [any other key for no]? |
```

Preview of the software

```
Do you want to continue [Pres `y` for yes] [any other key for no]? y


Enter the message you want to encrypt/decrypt: KnOz, lzkz, lzhz

Enter 1 for linear.
Enter 2 for rational.
Enter 3 for cubic.
Enter 4 for cubic root.

Enter your choice:
```

User needs to know the inverse function at this point. In our case $f^{-1}(x) = \frac{1}{3}x - \frac{1}{3}$

Preview of the software

```
Enter your choice: 1

Remember that a Linear Function has the form
                        a        c
              f(x) = --- x + ---
                        b        d

Enter the integer a: 1
Enter the integer b: 3

Enter the integer c: -1
Enter the integer d: 3

The new message is: Veni, vidi, vici


Do you want to continue [Pres `y` for yes] [any other key for no]?
```

Let's Decrypt Some Messages!

1. In groups, find all four inverse functions.
2. After all inverse functions have been found, send a pair from your group to the computer to enter one message and its inverse function.
3. When you receive your decrypted message, copy it on your paper, copy it on the board for the class to see, and return to your group.
4. As each pair returns, send out a new pair to decrypt and record.

Class Results: Excerpt # 1

1A: Once upon a midnight dreary, while
1B: I pondered, weak and weary, Over
1C: many a quaint and curious
1D: volume of forgotten lore- While
1E: I nodded, nearly napping, suddenly
1F: there came a tapping, As
1G: of some one gently rapping,
1H: rapping at my chamber door.

- What is the name of this poem?
-
- Who is author?
-

Class Results: Excerpt # 1

1A: Once upon a midnight dreary, while
1B: I pondered, weak and weary, Over
1C: many a quaint and curious
1D: volume of forgotten lore- While
1E: I nodded, nearly napping, suddenly
1F: there came a tapping, As
1G: of some one gently rapping,
1H: rapping at my chamber door.

- What is the name of this poem?
- The Raven.
- Who is author?
- Edgar Allan Poe.

Class Results: Excerpt # 2

2A: In the meantime it was folly to
2B: grieve, or to think. The prince had
2C: provided all the appliances of pleasure.
2D: There were buffoons, there were improvisatory,
2E: there were ballet dancers, there were
2F: musicians, there was Beauty, there was
2G: wine. All these and security were
2H: within. Without was the "Read Death."

- What is the title of this story?
-
- Who is author?
-

Class Results: Excerpt # 2

2A: In the meantime it was folly to
2B: grieve, or to think. The prince had
2C: provided all the appliances of pleasure.
2D: There were buffoons, there were improvisatory,
2E: there were ballet dancers, there were
2F: musicians, there was Beauty, there was
2G: wine. All these and security were
2H: within. Without was the "Read Death."

- What is the title of this story?
- The Masque of the Red Death.
- Who is author?
- Edgar Allan Poe.

Class Results: Excerpt # 3

3A: She was a child and I
3B: was a child, In this kingdom
3C: by the sea; But we loved
3D: with a love which was more
3E: than love- I and my
3F: Annabel Lee- With a love
3G: that the winged seraphs of
3H: heaven coveted her and me.

- What is the name of this poem?
-
- Who is author?
-

Class Results: Excerpt # 3

3A: She was a child and I
3B: was a child, In this kingdom
3C: by the sea; But we loved
3D: with a love which was more
3E: than love- I and my
3F: Annabel Lee- With a love
3G: that the winged seraphs of
3H: heaven coveted her and me.

- What is the name of this poem?
- Annabele Lee.
- Who is author?
- Edgar Allan Poe.

Class Results: Excerpt # 4

4A: These characters, as any one might readily
4B: guess, form a cipher- that is to
4C: say, they convey a meaning... I made
4D: up my mind, at once, that
4E: this was of a simple species-
4F: such, however, as would appear, to
4G: the crude intellect of the sailor,
4H: absolutely insoluble without the key.

- What is the name of this story?
-
- Who is author?
-

Class Results: Excerpt # 4

4A: These characters, as any one might readily
4B: guess, form a cipher- that is to
4C: say, they convey a meaning... I made
4D: up my mind, at once, that
4E: this was of a simple species-
4F: such, however, as would appear, to
4G: the crude intellect of the sailor,
4H: absolutely insoluble without the key.

- What is the name of this story?
- The Gold Bug.
- Who is author?
- Edgar Allan Poe.

Poe's Challenge

- 1839
- Issued to readers of the *Alexander's Weekly Messenger*
- Poe could solve any simple substitution cipher they cared to submit to him.
  - "It would be by no means a labor lost to show how great a degree of rigid method enters into enigma-guessing. This may sound oddly; but it is not more strange than the well known fact that rules really exist, by means of which it is easy to decipher any species of hieroglyphically writing -- that is to say writing where, in place of alphabetical letters, any kind of marks are made use of at random. For example, in place of A put % or any other arbitrary character --in place of B, a *, etc., etc. Let an entire alphabet be made in this manner, and then let this alphabet be used in any piece of writing. This writing can be read by means of a proper method. Let this be put to the test. **Let any one address us a letter in this way, and we pledge ourselves to read it forthwith--however unusual or arbitrary may be the characters employed.** "

See [4].

Poe's Challenge

- He correctly solve all submissions from December 1839 to May 1840.
  - Approximately 34 submissions. See [3].
- **The Gold Bug**.
  -Read Poe's famous story
  - Free copy from The Oxford Text Archive at `http://ota.ahds.ac.uk/`

References

[1]J.B. Fraleigh, *A First Course in Abstract Algebra*, 7th ed., Addison Wesley, NY, USA, 2002, page 181.

[2]http://questgarden.com/62/15/1/080310122438/process.htm, July 2011.

[3]http://oerrecommender.org/visits/13032, July 2011.

[4]C.S. Brigham, *Edgar Allan Poe's Contributions to Alexander's Weekly Messenger*, American Antiquarian Society, 1943.

Questions?

Any suggestions or comments, please let us know.

Thank you!

lharden6@stlcc.edu
junesl@uscsumter.edu