Cryptology Through History & Inquiry

Chuck Rocca
roccac@wcsu.edu

Western Connecticut State University

NES/MAA
Spring 2017 Meeting

NORWICH
200

June 2-3, 2017

https://goo.gl/q0HPP8

Outline

- Cryptology, History, and Math ...
- MathBook XML
- CTH&I
- Authoring while teaching

Cryptology, History, and Math ...

- Previous Observations

Cryptology, History, and Math ...

- Previous Observations
- This Semester's Goals

Cryptology, History, and Math ...

- Previous Observations
- This Semester's Goals
- Why LaTeX Wouldn't Cut It

Outline

- Cryptology, History, and Math ...
- MathBook XML
- CTH&I
- Authoring while teaching

MathBook XML

- What It Is

MathBook XML

- What It Is
  - Easy Accessability

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises
  - Click Here For Sample HTML

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises
  - Click Here For Sample HTML
  - Click Here For WeBWorK Sample HTML

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises
  - Click Here For Sample HTML
  - Click Here For WeBWorK Sample HTML
- A Brief Sample of Code

Sample Code

```
<?xml version="1.0" encoding="UTF-8"?>

<mathbook>

<!-- \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
            Header Information
     \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ -->

<docinfo>

    <!-- the other option is "long" which will produce an -->
    <!-- entire front matter section with more headings   -->
    <!-- <author-biographies length="short" /> -->

    <brandlogo url="https://sites.google.com/site/nesmaaspring2017meeting/" source="round_maa_logo.png" />

    <!-- Prefix to enhance Sage notebook contents -->
    <!-- <initialism>AATA</initialism> -->
    <!-- tikz package and libraries for images -->
    <!--
    Extra packages, package options, and package settings for latex-based images.
    Inserted in the preamble for LaTeX output.
    Inserted in the preamble to each standalone latex-based image for HMTL SVG output.
    <latex-image-preamble>
        \usepackage{pgfplots}           % loads tikz package
        \usepackage{smartdiagram}       % for a circular diagram
        \pgfplotsset{axis x line = middle,
                     axis y line = middle}
        \usetikzlibrary{backgrounds}
        \usetikzlibrary{arrows,matrix}
    </latex-image-preamble>
    <images>
        <archive from="charts_tables">svg png pdf</archive>
    </images>
</docinfo>
```

Sample Code

```
<!-- \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
            Start of Article
     \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ -->

    <article xml:id="NES_Sample">
        <title>Northeastern Section Meeting Sample Article</title>

<!-- \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
            Section 1: Some text
     \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ -->

        <section xml:id="basics">
            <title>Basic Text</title>
            <p>
            The purpose of this file is to let you see what a document typeset in Mathbook XML looks like.  This is by no means
            a complete sample of all of the possibilities of this system.
            </p>
            <definition>
                <title> RSA Encryption System </title>
                <statement>
                <p>
                Given two primes <m>p</m> and <m>q</m> we encipher a message <m>M</m> using the
                <term>RSA Encryption System</term> by calculating
                <me>
                    C\equiv M^e \pmod{n}
                </me>
                where <m>n=p\cdot q</m> and <m>e</m> is the public enciphering key which must be
                relatively prime to <m>\phi(n)</m>.
                </p>
                </statement>
            </definition>
        </section>

<!-- \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
```

Slide 1 (lines 89–130):

```xml
<section xml:id="images">
  <title>Images</title>
  <p>Inserting an image with a pre-existing image file:</p>
  <figure xml:id="appendix_figure_pigpen">
    <caption>Pigpen Cipher Key</caption>
    <image width="40%" source="images/Pigpen.png" archive="svg png pdf">
      <description> Cipher Key for the Pigpen Cipher </description>
    </image>
  </figure>

  <p>Inserting images with the picture environment or tikz:</p>
  <figure xml:id="appendix_figure_rSDES">
    <caption>Really Simple DES</caption>
    <image width="50%" archive="svg png pdf">
      <description>Part of a diagram for rSDES</description>
      <latex-image-code>
        <![CDATA[\begin{tikzpicture}
        \draw (0,0) node[above] {$M$};
        \draw[->] (0,0) -- (0,-2) node[below] {$IP$=[2,6,3,1,4,8,5,7]};
        \draw[->] (0,-2.5) -- (-2,-4) node[below] {$L_0$};
        \draw[->] (0,-2.5) -- (2,-4) node[below] {$R_0$};
        \draw[->] (2,-4.5) -- (-2,-6) node[below] {$L_1=R_0$};
        \draw[->] (-2,-4.5) -- (2,-6) node[below] {$R_1=L_0\oplus f(R_0,K_0)$};
        \draw[->] (2,-6.5) -- (-2,-8) node[below] {$L_2=L_1\oplus f(R_1,K_1)$};
        \draw[->] (2,-6.5) -- (2,-8) node[below] {$R_2=R_1$};
        \draw[->] (-2,-8.5) -- (-0.1,-10) node[below] {$IP^{-1}$=[4,1,3,5,7,2,8,6]};
        \draw[->] (2,-8.5) -- (0.1,-10);
        \draw[->] (0,-10.5) -- (0,-12) node[below] {$C$};
        \end{tikzpicture}]]>
      </latex-image-code>
    </image>
  </figure>

  <p>Inserting an instructional video from YouTube:</p>
  <figure xml:id="suzuki_vigenere_video">
    <caption>Modern look at the Vigenère Cipher</caption>
    <video youtube="SISnCm4_V-Y" width="80%"/>
  </figure>
</section>
```

Slide 2 (lines 259–300):

```xml
<paragraphs>
  <p>Final Message:</p>
  <blockquote>
    <p><c><scriptsize\triangle</c> EUS HJY TXZ UPE ISE QML COP BEN KVI WHO RRG OTD FL NEG OA</p>
  </blockquote>
</paragraphs>
<p>
  Reflection Questions:
  <ol>
    <li>
      Looking at <xref ref="falconer_trans_table_2" autoname="yes"/> why is <em>the</em>
      from the beginning of the sentence written backwards? (Be sure to look carefully at the
      letters to the left of the row when answering.)
    </li>
    <li>
      In the second row of the same table why is <em>qui</em> from <em>quick</em> is
      written in the order it is written?
      (Again, be sure to look carefully at the letters to the left of the row when answering.)
    </li>
    <li>
      In the last row we put down <em>o</em> from <em>brown</em> and the <em>fo</em> from <em>fox</em>, why are they in the
      order they are in and looking at the next table (<xref ref="falconer_trans_table_3" autoname="yes" />) where do we put
      the <em>x</em> from <em>fox</em> and why?
    </li>
    <li>
      How do we finish writing the rest of the message into the boxes in the table?
    </li>
    <li>
      Reflection Questions:
      Looking at the final message why is there a little triangle at the start of the message and why
      were the blocks of letters written in the order they were written?
    </li>
    <li>
      In what ways is this different from other ciphers we have looked at? (Hint: in this cipher what does
      cipher text <em>E</em> represent, or cipher text <em>f</em>?)
    </li>
  </ol>
</p>
</subsection>
<subsection>
  <title>Decrypting the Transposition:</title>
```

Slide 3 (lines 183–218):

```xml
Let's see if you can follow Falconer's directions. Below I set up <xref ref="falconer_trans_table_1" autoname="yes"/> according
his description in steps (5) and (6) and used it to encipher the pangram<index><main>pangram</main></index> <em><q>the quick brown
fox jumps over the lazy sleeping dog.</q></em>
</p>

<table xml:id="falconer_trans_table_1">
  <caption> Falconer's Transposition Table Initial Setup</caption>
  <tabular top="minor" left="minor" right="minor" halign="center" bottom="minor">
    <row>
      <cell /><cell> </cell><cell>A</cell><cell>B</cell><cell>C</cell>
    </row>
    <row>
      <cell>1</cell><cell>CBA</cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell>
    </row>
    <row>
      <cell>2</cell><cell>CAB</cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell>
    </row>
    <row>
      <cell>3</cell><cell>ACB</cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell>
    </row>
    <row>
      <cell>4</cell><cell>BCA</cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell>
    </row>
    <row>
      <cell>5</cell><cell>BAC</cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell><cell><p>\phantom{WRW}</p></cell>
    </row>
  </tabular>
</table>
<table xml:id="falconer_trans_table_2">
  <caption> Falconer's Transposition Table First Pass</caption>
  <tabular top="minor" left="minor" right="minor" halign="center" bottom="minor">
    <row>
      <cell /><cell> </cell><cell>A</cell><cell>B</cell><cell>C</cell>
    </row>
    <row>
      <cell>1</cell><cell>CBA</cell><cell>E</cell><cell>H</cell><cell>T</cell>
    </row>
  </tabular>
```

Slide 4 (lines 495–537):

```python
<section xml:id="sage">
  <title>Sage Incorporation</title>
  <p>Falconer Cipher Cell:</p>
  <sage xml:id="sage_falconer_cell">
    <input>

<!-- Python/Sage Function -->
import textwrap
import re
@interact
def falconer(message=input_box("The quick brown fox jumps over the lazy sleeping dog.",
                label="Message:", type=str, width=50, height=3),
            keys=input_grid(1,6,default=["CBA", "CAB", "ACB", "BCA", "BAC",""],
                label="Keys:", to_value=list, type=str),
            chars=[3..5]):
    text = re.sub("[^A-Z]",''
        ,str(message.encode('ascii','replace')).upper())
    columns = "ABCDE"
    key = keys[0]
    while "" in key: key.remove("")
    message_table = [["" for x in range(chars)] for y in range(len(key))]
    for i in xrange(0,len(text),chars):
        row = (i//chars)%len(key)
        for j in range(chars):
            try:
                col = columns.index(key[row][j])
            except:
                col = chars-1 #pass
            try:
                message_table[row][col] += str(text[i+j])
            except:
                pass
    out_message = ""
    print "Characters in text: ",len(text)
    print "Cipher Table:"
    for k in range(len(key)):
        print "\t",str(key[k][0:chars]),":\t","\t".join(message_table[k])
        for i in range(chars):
            out_message += str(message_table[k][i])+" "
    print "Completed Message:"
    #for i in xrange(0,len(out_message),50):
    #    print "\t",out_message[i:min(i+50,len(out_message))].strip()
    print textwrap.fill(out_message, 50)
```

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises
  - Click Here For Sample HTML
  - Click Here For WeBWorK Sample HTML
- A Brief Sample of Code
  - Click Here For MBX

MathBook XML

- What It Is
  - Easy Accessability
  - Multiple Formats
  - Interactive Text
  - Interactive Exercises
  - Click Here For Sample HTML
  - Click Here For WeBWorK Sample HTML
- A Brief Sample of Code
  - Click Here For MBX
  - Click Here For HTML

Outline

- Cryptology, History, and Math ...
- MathBook XML
- CTH&I
- Authoring while teaching

CTH&I

- What I Managed To Do

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes
  - Ciphers after 1700 CE - 1928 CE - Not So Much

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes
  - Ciphers after 1700 CE - 1928 CE - Not So Much
  - Hill's Cipher - Yes

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes
  - Ciphers after 1700 CE - 1928 CE - Not So Much
  - Hill's Cipher - Yes
  - Post Hill - Not So Much

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes
  - Ciphers after 1700 CE - 1928 CE - Not So Much
  - Hill's Cipher - Yes
  - Post Hill - Not So Much
  - Click Here For HTML

CTH&I

- What I Managed To Do
  - Ciphers from 50 BCE - 1700 CE - Yes
  - Ciphers after 1700 CE - 1928 CE - Not So Much
  - Hill's Cipher - Yes
  - Post Hill - Not So Much
  - Click Here For HTML
  - Click Here For PDF

CTH&I

- How It Could Be Used

CTH&I

- How It Could Be Used
  - Standard text

CTH&I

- How It Could Be Used
  - Standard text
  - Out of class supplement

CTH&I

- How It Could Be Used
  - Standard text
  - Out of class supplement
  - Source for guided inquiry

CTH&I

- What Still Needs To Be Done

CTH&I

- What Still Needs To Be Done
  - Clean up formatting

CTH&I

- What Still Needs To Be Done
  - Clean up formatting
  - Fill in missing details

CTH&I

- What Still Needs To Be Done
  - Clean up formatting
  - Fill in missing details
  - Increase the ciphers covered

CTH&I

- What Still Needs To Be Done
  - Clean up formatting
  - Fill in missing details
  - Increase the ciphers covered
  - Find additional original sources

CTH&I

- What Still Needs To Be Done
  - Clean up formatting
  - Fill in missing details
  - Increase the ciphers covered
  - Find additional original sources
  - Add interactivity (but with a cautionary comment on technology)

Outline

- Cryptology, History, and Math ...
- MathBook XML
- CTH&I
- Authoring while teaching

Authoring While Teaching

- Motivation

Authoring While Teaching

- Motivation
- Scrambling

Authoring While Teaching

- Motivation
- Scrambling
- Should You Do It?

Authoring While Teaching

- Motivation
- Scrambling
- Should You Do It? Ehhhh...

Cryptology Through History & Inquiry

Chuck Rocca
roccac@wcsu.edu

Western Connecticut State University

June 2-3, 2017