Cryptology Through History & Inquiry

Chuck Rocca
roccac@wcsu.edu

Western Connecticut State University

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>

<!-- %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

Sample Code

```
89
90          <section xml:id="images">
91              <title>Images</title>
92              <p>Inserting an image with a pre-existing image file:</p>
93              <figure xml:id="appendix_figure_pigpen">
94                  <caption>Pigpen Cipher Key</caption>
95                  <image width="40%" source="images/Pigpen.png" archive="svg png pdf">
96                      <description> Cipher Key for the Pigpen Cipher </description>
97                  </image>
98              </figure>
99
100             <p>Inserting images with the picture environment or tikz:</p>
101             <figure xml:id="appendix_figure_rSDES">
102                 <caption>Really Simple DES</caption>
103                 <image width="60%" archive="svg png pdf">
104                     <description>Part of a diagram for rSDES</description>
105                     <latex-image-code>
106                         <![CDATA[\begin{tikzpicture}
107
108                             \draw (0,0) node[above] {$M$};
109                             \draw[->] (0,0) -- (0,-2) node[below] {$IP$=[2,6,3,1,4,8,5,7]};
110                             \draw[->] (0,-2.5) -- (-2,-4) node[below] {$L_0$};
111                             \draw[->] (0,-2.5) -- (2,-4) node[below] {$R_0$};
112                             \draw[->] (2,-4.5) -- (-2,-6) node[below] {$L_1=R_0$};
113                             \draw[->] (-2,-4.5) -- (2,-6) node[below] {$R_1=L_0\oplus f(R_0,K_0)$};
114                             \draw[->] (-2,-6.5) -- (-2,-8) node[below] {$L_2=L_1\oplus f(R_1,K_1)$};
115                             \draw[->] (2,-6.5) -- (2,-8) node[below] {$R_2=R_1$};
116                             \draw[->] (-2,-8.5) -- (-0.1,-10) node[below] {$IP^{-1}$=[4,1,3,5,7,2,8,6]};
117                             \draw[->] (2,-8.5) -- (0.1,-10);
118                             \draw[->] (0,-10.5) -- (0,-12) node[below] {$C$};
119
120                         \end{tikzpicture}]]>
121                     </latex-image-code>
122                 </image>
123             </figure>
124
125             <p>Inserting an instructional video from YouTube:</p>
126             <figure xml:id="suzuki_vigenere_video">
127                 <caption>Modern look at the Vigen&#x00E8;re Cipher</caption>
128                 <video youtube="5ISnCm4_V-Y" width="80%"/>
129             </figure>
130         </section>
```

Sample Code

```
259                 <paragraphs>
260                     <p>Final Message:</p>
261                     <blockquote>
262                         <p><q><m>\scriptsize\triangle</m> EUS HJY TXZ UPE ISE QML COP BEN KVI WHO RRG OTD FL NEG OA</q></p>
263                     </blockquote>
264                 </paragraphs>
265                 <p>
266                     Refection Questions:
267                     <ul>
268                         <li>
269                             Looking at <xref ref="falconer_trans_table_2" autoname="yes"/> why is <em>the</em>
270                             from the beginning of the sentence written backwards? (Be sure to look carefully at the
271                             letters to the left of the row when answering.)
272                         </li>
273                         <li>
274                             In the second row of the same table why is <em>qui</em> from <em>quick</em>
275                             written in the order it is written?
276                             (Again, be sure to look carefully at the letters to the left of the row when answering.)
277                         </li>
278                         <li>
279                             In the last row we put down <em>n</em> from <em>brown</em> and the <em>fo</em> from <em>fox</em>, why are they in the
280                             order they are in and looking at the next table (<xref ref="falconer_trans_table_3" autoname="yes" />) where do we put
281                             the <em>x</em> from <em>fox</em> and why?
282                         </li>
283                         <li>
284                             How do we finish writing the rest of the message into the boxes in the table?
285                         </li>
286                         <li>
287                             Refection Questions:
288                             Looking at the final message why is there a little triangle at the start of the message and why
289                             were the blocks of letters written in the order they were written?
290                         </li>
291                         <li>
292                             In what ways is this different from other ciphers we have looked at?  (Hint: in this cipher what does
293                             cipher text <em>E</em> represent, or cipher text <em>F</em>?)
294                         </li>
295                     </ul>
296                 </p>
297             </subsection>
298             <subsection>
299                 <title>Decrypting the Transposition</title>
300                 <p>
```

Sample Code

```
183                 Let's see if you can follow Falconer's directions.  Below I set up <xref ref="falconer_trans_table_1" autoname="yes"/> accordin
                    his description in steps (5) and (6) and used it to encipher the pangram<index><main>pangram</main></index> <em><q>the quick br
                    fox jumps over the lazy sleeping dog.</q></em>
184             </p>
185
186             <table xml:id="falconer_trans_table_1">
187                 <caption> Falconer's Transposition Table Initial Setup</caption>
188                 <tabular top="minor" left="minor" right="minor" halign="center" bottom="minor">
189                     <row>
190                         <cell /><cell> </cell><cell>A</cell><cell>B</cell><cell>C</cell>
191                     </row>
192                     <row>
193                         <cell>1</cell><cell>CBA</cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}<
                            cell>
194                     </row>
195                     <row>
196                         <cell>2</cell><cell>CAB</cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}<
                            cell>
197                     </row>
198                     <row>
199                         <cell>3</cell><cell>ACB</cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}<
                            cell>
200                     </row>
201                     <row>
202                         <cell>4</cell><cell>BCA</cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}<
                            cell>
203                     </row>
204                     <row>
205                         <cell>5</cell><cell>BAC</cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}</m></cell><cell><m>\phantom{WRW}<
                            cell>
206                     </row>
207                 </tabular>
208             </table>
209             <table xml:id="falconer_trans_table_2">
210                 <caption> Falconer's Transposition Table First Pass</caption>
211                 <tabular top="minor" left="minor" right="minor" halign="center" bottom="minor">
212                     <row>
213                         <cell /><cell> </cell><cell>A</cell><cell>B</cell><cell>C</cell>
214                     </row>
215                     <row>
216                         <cell>1</cell><cell>CBA</cell><cell>E</cell><cell>H</cell><cell>T</cell>
217                     </row>
218                     <row>
```

Sample Code

```
        <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 "Chracters 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