

A tale of two cryptology courses and an open source textbook

Tamara B. Veenstra

University of Redlands

January 24, 2023

My Background

- Teaching for 26 years: 22 at University of Redlands, 4 at University of Northern Iowa
- Background mathematical area: number theory
- Taught my first crypto course in 2000 (honors non-major seminar)
- Many variations since then; two main flavors
- Supervised many senior projects in cryptology (undergraduate, expository)
- Started to wonder what research in the area was like
- Summer SCAMP program at The Center for Communications Research in La Jolla (classified research) [2007]

Goal 1

- I love teaching cryptology courses!
- Students get so excited about the topic.
- I have designed lots of materials over the years.
- I would love to share them.
- Before I leave academia.
- In June.
- For full time work in crypto research. (sabbatical fail?)

Goal 2

- I bet others also love teaching cryptology courses!
- And would be happy to share activities and ideas.
- How can we help support each other in our classes?

Overview

- Overview of the two main flavors of courses that I teach.
- An open education resource textbook for math major version.
- Some of my favorite activities in each, mostly the general audience one.
- Discussion about how we support each other as a crypto educators community, how to share resources.
- But please feel free to ask questions and make comments as we go!

Flavor One: Math Majors and Minors

- Sophomore level math major and minor
- Transition to higher mathematics course
- Intensive term format (3 hours/day, 4 days/week)
- Discovery and guided inquiry based (3 hours/day)
- Focus on exploration and making conjectures
- Sage Math component for computations via interactive Sage cells

Flavor One: Topics

- Monoalphabetic Ciphers (shift, affine, general, modular arithmetic)
- Polyalphabetic Ciphers (Vigenère, Enigma)
- Public Key Cryptography (Diffie-Helman, RSA)
- Block Ciphers (Playfair, Hill)
- Mostly historical (plus mathematical) ordering.
- Exception: public key too much for last week of class.

Writing a Textbook

- Wanted discovery and exploration based (not enough in most crypto texts)
- Needed organization of many Sage Math interactive cells
- Textbooks are expensive (DEI issues)
- Solution: write my own textbook using PreText software (<https://pretextbook.org/>)
- Open Educational Resources (online text + source code (soon))

The Textbook

- <http://tamarabveenstra.com/CryptologyTextbook/>
- Example: http://facweb1.redlands.edu/fac/Tamara_Veenstra/cryptobook/enigma-history.html
- Activities are all built into the textbook. (Investigations)
- (Solutions are not.)

Goal 3

- I would love for others to use any part of this textbook.
- Once source code is posted, can be modified to create your own textbook. (Creative Commons Attribution-ShareAlike License.)
- Feedback, suggestions, and collaborations are welcome!
- Some complications. (pre-pub issues)
- Funny story

Flavor Two

- General audience level course
- Interdisciplinary
- First year seminar or Senior honors seminar

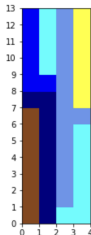
Flavor Two: Topics (Senior honors version)

- Monoalphabetic ciphers (Sherlock Holmes stories)
- Culper Spy Ring (Turn TV series)
- Steganography: Invisible Ink and Grills/Masks
- Transposition ciphers, Civil War era and Cardano Grills
- Elizebeth Smith Friedman (biographies/unfinished memoir link)
- Cipher Quilt
- Women Code Breakers in WWII (Code Girls by Liza Mundy)
- Blockchain and Zero Knowledge Protocols (Bubble or Revolution)

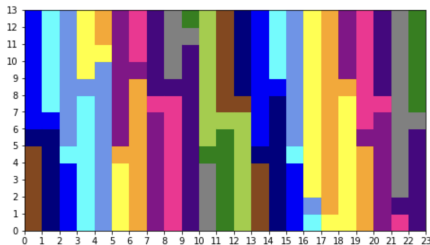
A few of my favorite things

- Secret Ink (helps to have a friendly chemist) link to video
- Cipher Quilt: Designed by Maureen Quirk

HINT:



Cipher quilt



- Code Girls Discussion on gender roles and issues
- Unessay Final Project (any topic and any method of presentation/engagement)

Freeform Final Projects

- Unessay Link
- Crochet cipher, Knit ciphers
- Presentation on Ciphers and Serial Killers (Zodiac, BTK)
- Cryptography inspired make-up packaging (3D printed)
- Legal argument about encryption and fourth amendment
- The Wassenaar Arrangement simulation (about export controls and encryption)
- Five fictional letters of women in cryptology from different eras writing to each other (with a method of encryption for each letter)
- ArcGIS StoryMap: Environmental impact of blockchain techno
- Electronic cipher challenge/scavenger hunt (google forms, wikipedia, automated email responses, etc)

Crochet blanket and Make-up Packaging



MESSAGE: SCU
POWDER COMPACTS

CRYPTOS

CODE
BLUSH

MESSAGE:
SCU DPR RGW
OPS EOA FEL WB

FOR
INSTRUCTIONS ON
USE SOLVE USING
A TRANSPOSITION
CIPHER.

KRYPTOSBEAUTY.COM

Scavenger Hunt

Follow these steps to find the Doordash code.

1. Complete one of these puzzles. They are timed. You only need to succeed once. If you fail, attempt the next one.

<https://test.gclocked.com/?form=-NHph40rMJzwbWXCy0-B>

https://test.gclocked.com/?form=-NHpjNU8eHy_GoLBi9kw

<https://test.gclocked.com/?form=-NHpkd8BJ9g4XW1dUWnS>

1. Upon a correct answer, follow the next step to find the address key
2. Input address key into the blank. Send any message to the address and await response.

Address: _____ 1812@ [gmail.com](#)

Cypher 2

[Sign in to Google](#) to save your progress. [Learn more](#)

* Required

rfehaleccpeinir

Your answer

Google Forms Response: 4:31, 1:5

Wikipedia article for Rail Fence Cipher: 4th topic, 31st word

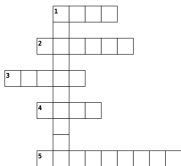
Crossword Labs

[Make a Crossword](#) [Find a Crossword](#) [About](#) [Login/Sign Up](#)

cryptographer crossword

[Share](#) [Focus Mode](#) [Print](#)

[Instructions](#) | [Embed](#) | [Edit](#)



Discussion

- Any questions?
- Is there a good way to share course materials with each other?
- What course materials would be helpful? Syllabus bank? Notes? Activities? Homework sets?
- What courses or materials have others developed?

Thank You!

Feel free to reach out to discuss more!

Slides available at:

http://tamarabveenstra.com/Talks/crypto_ed_jan23.pdf

tamara_veenstra@redlands.edu (until May 31, 2023)

-or-

tamarabveenstra@gmail.com (permanent)