Classical Cryptography

Introduction: a puzzling matter?

Karst Koymans

Informatics Institute
University of Amsterdam
(version 22.4, 2023/02/06 10:41:38 UTC)

Tuesday, February 7, 2023

Table of Contents

Organisation

- Information is available on
  - The OS3 Website/Wiki
    - For the first three weeks
    - `https://www.os3.nl/2022-2023/courses/crypto/start`
  - Canvas
    - For the remainder of the course
    - `https://canvas.uva.nl/courses/36021`
- Lectures
- Practical exercises
- Programming exercises

Lectures 1

- The course will be divided in two parts
- Part I
  - Lecturer Karst Koymans
  - February 7 — February 24
- Part II
  - Lecturer Taco Walstra
  - February 28 — March 20
- Q&A session for both parts on March 24

Lectures 2

- Seven weeks
- February 7 — March 24
  - Tuesday, 11:00-13:00, SP D1.111
    - Tuesday, March 14 and 21, will be moved to **Monday**, March 13 and 20, 11:00-13:00, **SP C0.05**
  - Friday, 11:00-13:00, SP D1.111
    - Friday, March 17 and 24, 11:00-13:00, **SP L1.01**

Guest Lecture

- **Enigma**
  - Jaap van Ginkel
  - Tuesday, February 28

Practical and "programming" exercises

- February 7 — March 24
  - Tuesday, 13:00-15:00, SP D1.111
    - Tuesday, March 14 and 21, will be moved to **Monday**, March 13 and 20, 13:00-15:00, in SP D1.111
  - Friday, 13:00-15:00, SP D1.111
- Teaching assistants
  - **Kyrian Maat**, **Rick Klarenberg**, **Stijn Maatje**, **Taco Walstra**
- Programming language used is **Ruby**
  - You may replace it by something of your **own choice**
  - This is **not** a programming course
  - The programs are only **tools** supporting your cryptanalysis

Homework and support

- Homework
  - Via assignments/quizzes in Canvas
  - Graded by the teaching assistants
- Support
  - Discussions in Canvas
  - We are not available 24/7

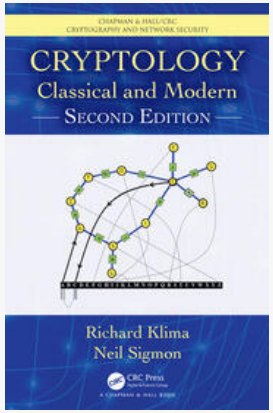
Judgment

- The final grading is determined by
  - **Homework assignments** (20 %)
  - **On-site written exam** (80 %)
- Primary learning material
  - (Referenced parts of) **Cryptology, Classical and Modern**
  - **Slides** from the lectures
- Secondary learning material
  - Referenced parts of Hans van der Meer's **syllabus**
  - Material that can reasonably be expected to be known from practical and programming **exercises**

Exam dates

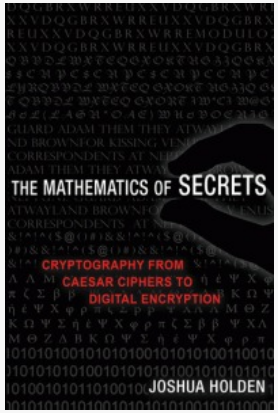
- Classical Cryptography **exam** will be on
  - Wednesday, March 29, 13:00-16:00, REC C1.04
- Classical Cryptography **resit** will be on
  - Friday, June 2, 11:00-14:00, SP D1.116

Book



- **Cryptology**: Classical and Modern, 2nd edition
- Richard Klima and Neil Sigmon
- ISBN-13: 9781138047624
- `https://www.routledge.com/Cryptology-Classical-and-Modern-Second-Edition/Klima-Sigmon/p/book/9781138047624`

Auxiliary book

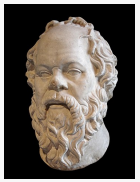


- **The Mathematics of Secrets**: Cryptography from Caesar Ciphers to Digital Encryption
- Joshua Holden
- ISBN-13: 9780691141756 (hardcover)
- ISBN-13: 9780691183312 (paperback)
- `http://mathofsecrets.com/` (`https://mathofsecrets.com/?`)

Some advice

- Keep up with theory and practice **right from the start**
- **Read** the book (like in a "flipped classroom")

The only true wisdom is in knowing you know nothing



—Socrates

Basic terminology

cryptology cryptography plus cryptanalysis

cryptography secret writing

- from ancient Greek κρυπτός: concealed, hidden, secret
- steganography is hidden writing
  - from ancient Greek στεγανός: covered, concealed

cryptanalysis (unauthorised) reading of a cryptogram

- or even discovering secret key(s), possibly only partially

Basic symmetric/secret scheme

$$C = \mathcal{E}(M, K)$$
$$M = \mathcal{D}(C, K)$$
$$M = \mathcal{D}(\mathcal{E}(M, K), K)$$

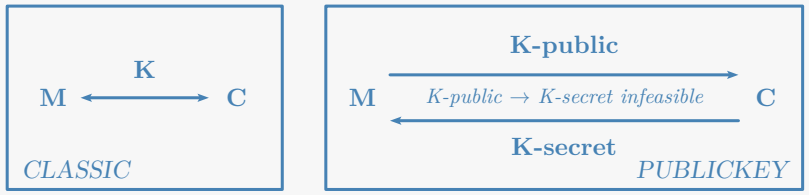
- $\mathcal{E}$ is encryption; $\mathcal{D}$ is decryption
- M is the message; C is the cryptogram; K is the secret key
- $\mathcal{E}(-, K)$ is injective for each K
- K has to be kept a secret, exclusively between any two communicating parties

Basic asymmetric/public scheme

$$C = \mathcal{E}(M, K_p)$$
$$M = \mathcal{D}(C, K_s)$$
$$M = \mathcal{D}(\mathcal{E}(M, K_p), K_s)$$

- $\mathcal{E}$ is encryption; $\mathcal{D}$ is decryption
- M is the message; C is the cryptogram; K's are two keys, one public, one secret
- $\mathcal{E}(-, K_p)$ is injective for each K_p
- K_s has to be kept a secret for each participant separately
- K_p must be known to all parties (in a **verifiable** way, for instance through a PKI)
  - PKI stands for Public Key Infrastructure

Symmetric versus asymmetric encryption



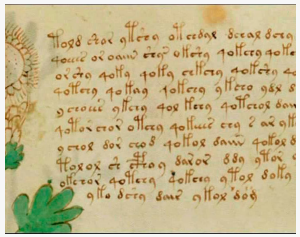
Kerckhoffs' rules (some of them are dated)

- The system must be practically, if not mathematically, indecipherable.
- **It should not require secrecy, and it should not be a problem if it falls into enemy hands.**
- It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will.
- It must be applicable to telegraph communications.
- It must be portable, and should not require several persons to handle or operate.
- Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Types of attack

- Increasing in usefulness of available information
  - Ciphertext-only ("Known-ciphertext")
  - Known-plaintext
  - Chosen-plaintext
  - Chosen-ciphertext
- Increasing in possible interaction
  - Passive (observation only)
  - Active (adaptation of messages)

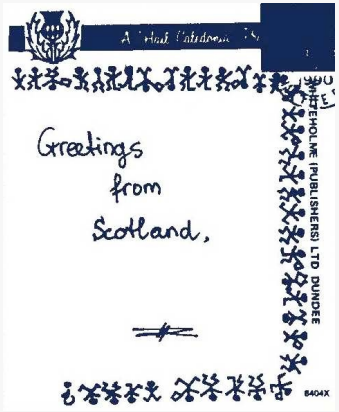
The Voynich manuscript



Real or fake? Decoded or not? Latest claims (not convincing[1])
Nicholas Gibbs (September 2017), Greg Kondrak (January 2018, using AI),
Ahmet Ardiç (2018), Gerard Cheshire (2019)

[1] This shows recent activity, but the results are much disputed. Some people have too much fantasy.

A personal message



Source: Hans van der Meer

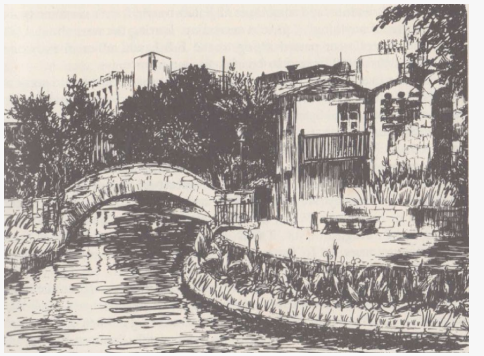
—

personal message

https://en.wikipedia.org/wiki/The_Adventure_of_the_Dancing_Men

https://www.arthur-conan-doyle.com/index.php?title=Dancing_Men_Alphabet

Just a picture?

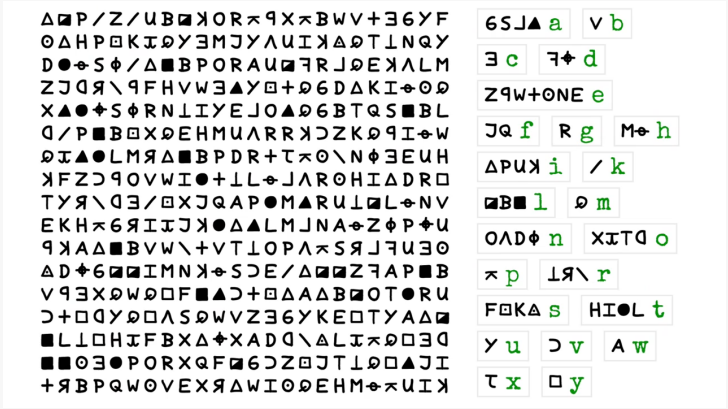


Source: https://scienceblogs.de/klausis-krypto-kolumne/2015/05/21/versteckte-nachrichten-in-modezeichnungen-grashalmen-und-apfelbaeumen/

The Zodiac Killer Z408 cryptogram (July 31, 1969)

Source: https://zodiackiller.fandom.com/wiki/408-cipher

The Z408 cryptogram solution (August 8, 1969)



Source: https://www.youtube.com/watch?v=57o8g3d6lSw

The Z408 cryptogram text (with spelling errors retained)

I like killing people because it is so much fun it is more fun than killing wild game in the forrest because man is the most dangeroue anamal of all to kill something gives me the most thrilling experence it is even better than getting your rocks off with a girl the best part of it is thae when I die I will be reborn in paradice and all the I have killed will become my slaves I will not give you my name because you will try to sloi down or atop my collectiog of slaves for my afterlife **ebeorietemethhpiti**

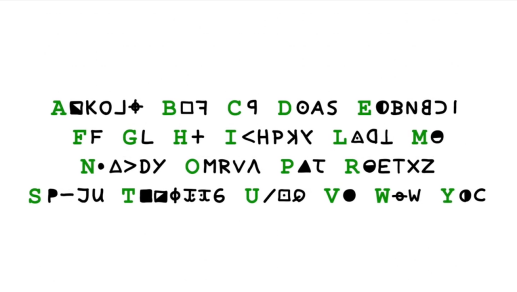
The Z340 cryptogram

The Z340 cryptogram from November 8, 1969

David Oranchak cracked Z340 with two colleagues on December 5, 2020

https://zodiacrevisited.com/reporting-on-the-zodiac-killer-ciphers/
https://www.youtube.com/watch?v=57o8g3d61Sw

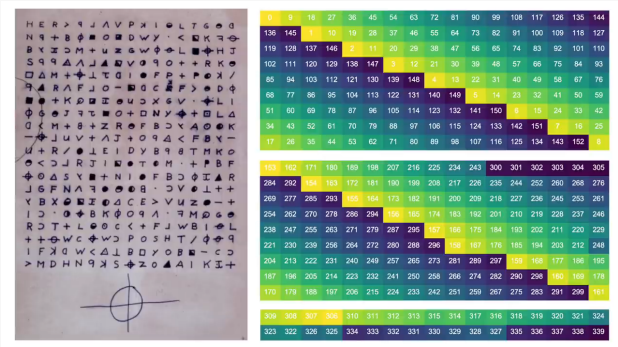
The Z340 cryptogram solution (substitution part)



This is the homophonic substitution part

Source: https://www.youtube.com/watch?v=-1oQLPRE21o

The Z340 cryptogram solution (transposition part)



This is the transposition part

Source: https://www.youtube.com/watch?v=-1oQLPRE21o

The Z340 cryptogram text (after spelling correction)

I hope you are having lots of fun in trying to catch me. That wasn't me on the TV show, which brings up a point about me. I am not afraid of the gas chamber because it will send me to paradise all the sooner, because I now have enough slaves to work for me where everyone else has nothing when they reach paradise, so they are afraid of death. I am not afraid because I know that my new life is life will be an easy one in paradise death.

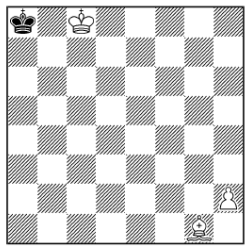
Why puzzling?

- Improves accuracy
- Sharpens your brain
- Forces thinking out of the box
- Uses your creativity
- Never a dull moment
- **I**mproves accuracy
- **S**harpens your brain
- **F**orces thinking out of the box
- **U**ses your creativity
- **N**ever a dull moment
- ...

This (and more) is important for cryptanalysts
Notice the **acrostic** (ἄκρος στίχος — topmost verse)

Puzzle 1: Chess retrograde analysis

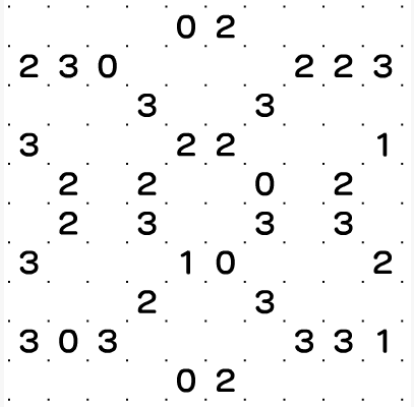
Smullyan



White to move. What was black's last move?

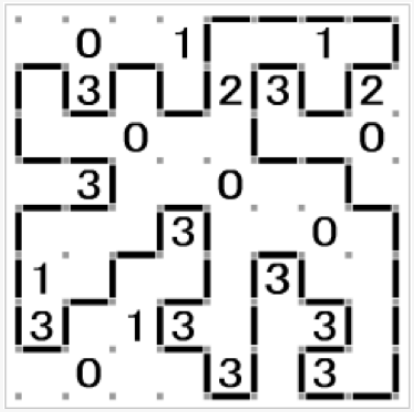
https://www.mathpuzzle.com/retrograde.html

Puzzle 2: Slitherlink



What are the rules of this game?

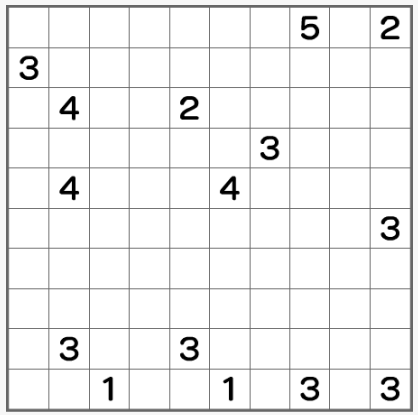
Puzzle 2: Slitherlink continued



Try it yourself

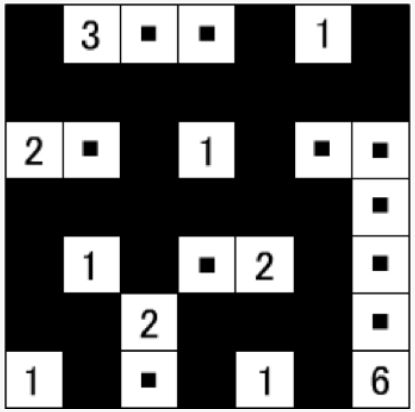
https://www.brainbashers.com/slitherlink.asp

Puzzle 3: Nurikabe



What are the rules of this game?

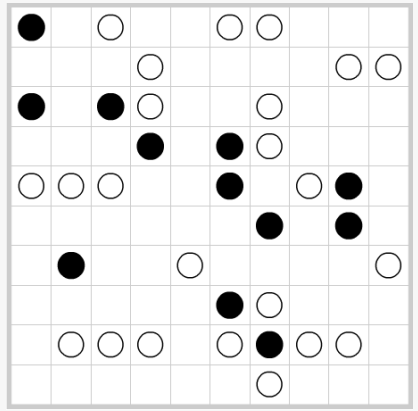
Puzzle 3: Nurikabe continued



Try it yourself

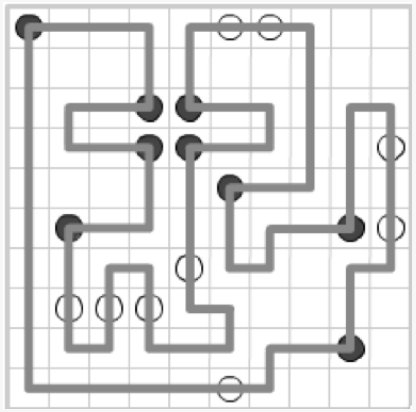
https://www.puzzle-nurikabe.com/

Puzzle 4: Masyu



What are the rules of this game?

Puzzle 4: Masyu continued



Try it yourself

https://www.interactive.onlinemathlearning.com/fun_pearl.php