Classical Cryptography

Introduction: a puzzling matter?

Karst Koymans

Informatics Institute

University of Amsterdam

(version 19.5, 2020/02/05 15:55:14 UTC)

Monday, February 3, 2020

1. Organisation
    - Global Structure
    - Lectures
    - Practical exercises
    - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Organisation

- Information available on the OS3 Website/Wiki
  - `https://www.os3.nl/2019-2020/courses/crypto/start`
- Lectures
- Practical exercises
- Programming exercises

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Lectures

- Seven weeks
- February 3 - March 19
    - Monday, 15:00-17:00, G0.10-G0.12
    - Thursday, 15:00-17:00
        - February 6 and March 19: A1.28
        - February 13: A1.04
        - February 20, 27 and March 5: G0.23-0.25
- **No lecture** on March 12
- Q&A session on March 19

Guest Lecture

- Monday, February 24
  - **Enigma**, by Hans van der Meer

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Practical and “programming” exercises

- Monday, 15:00-17:00, G0.10-G0.12
- Thursday, 15:00-17:00, G0.23-G0.25
- Lab assistant: **Felix Brakel**
- Programming language used is Ruby
  - You may replace it by something of your own choice
  - This is **not** a programming course
  - The programs are **tools** supporting cryptanalysis

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Judgment

- The final grading is only determined by the **written exam**
- Primary learning material
  - (Referenced parts of) Joshua Holden's **The Mathematics of Secrets**
  - **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**

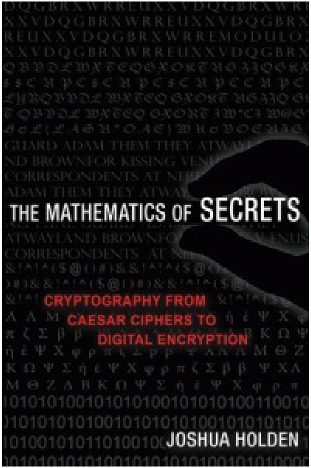
Exam dates

- Classical Cryptography **exam** will be on
  - Monday, March 23, 09:00-12:00, Science Park C0.05
- Classical Cryptography **resit** will be on
  - Tuesday, May 26, 18:00-21:00, Science Park D1.111

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Book


THE MATHEMATICS OF SECRETS
CRYPTOGRAPHY FROM CAESAR CIPHERS TO DIGITAL ENCRYPTION
JOSHUA HOLDEN

- **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/`?)

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

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

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

Basic terminology

cryptology cryptography plus cryptanalysis

cryptography secret writing

- steganography is hidden writing

cryptanalysis (unauthorized) reading of a cryptogram

- or even getting the key (possibly partially)
- or doing traffic analysis

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 key
- $\mathcal{E}(-, K)$ is injective for each K
- K has to be kept a secret between two communicating parties

Basic asymmetric/public scheme

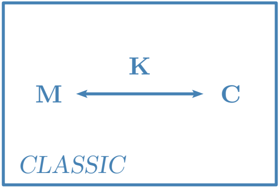
$$C = \mathcal{E}(M, K_p)$$

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

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

- $\mathcal{E}$ is encryption; $\mathcal{D}$ is decryption
- M is the message; C is the cryptogram; K's are two keys
- $\mathcal{E}(-, K_p)$ 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)

Symmetric versus asymmetric encryption

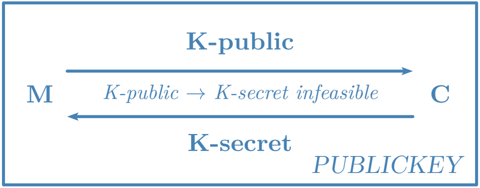


K

M

C

CLASSIC



K-public

M

K-public → *K-secret infeasible*

C

K-secret

PUBLICKEY

Kerckhoffs' rules

- 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.

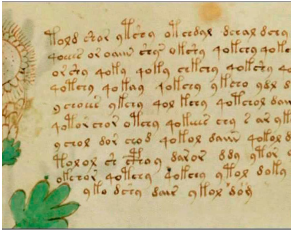
Types of attack

- Increasing in strength:
    - Ciphertext-only
    - Known-plaintext
    - Chosen-plaintext
    - Chosen-ciphertext
- From observation to interaction
    - Passive (observing only)
    - Active (changing messages)

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

The Voynich manuscript



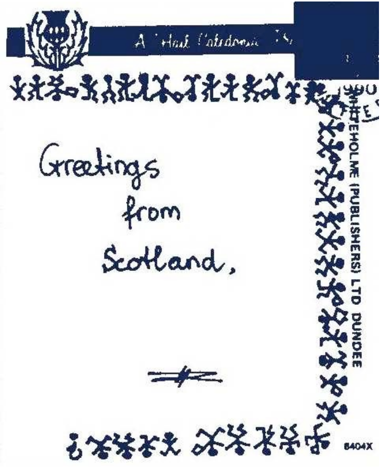
Real or fake?

Decoded or not?

Latest claims Nicholas Gibbs (September 2017)

and Greg Kondrak (January 2018, using AI)

A personal message

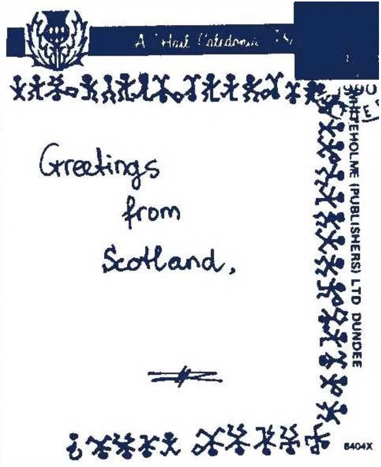


Source: Hans van der Meer

—

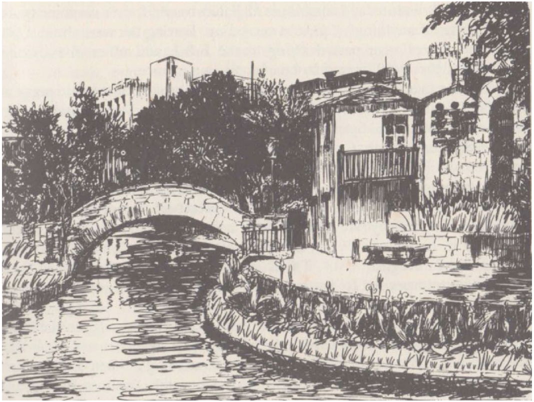
personal message

A personal message



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

Just a picture?



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

Outline

1. Organisation
   - Global Structure
   - Lectures
   - Practical exercises
   - Examination
2. Book
3. Advice
4. Basic concepts in cryptography
5. Some examples
6. Puzzling

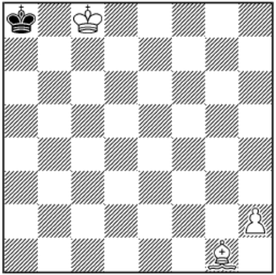
Why puzzling?

- Accuracy
- Brain training
- Creativity
- Having fun
- Out of the box
- ...

These are all important for cryptanalysts

Puzzle 1: Chess retrograde analysis

Smullyan



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

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

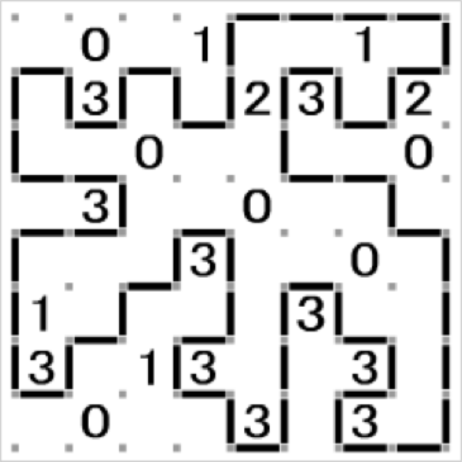
(https://www.mathpuzzle.com/retrograde.html?)

Puzzle 2: Slitherlink

				0	2				
2	3	0					2	2	3
			3			3			
3				2	2				1
	2		2			0		2	
	2		3			3		3	
3				1	0				2
			2			3			
3	0	3					3	3	1
				0	2				

What are the rules of this game?

Puzzle 2: Slitherlink continued



Try it yourself

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

Puzzle 3: Nurikabe

							5		2
3									
	4			2					
						3			
	4				4				
									3
	3			3					
		1			1		3		3

What are the rules of this game?

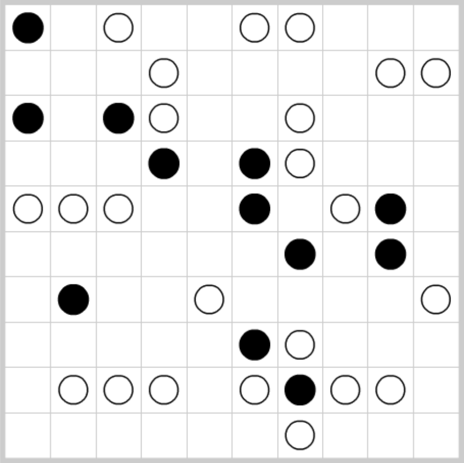
Puzzle 3: Nurikabe continued

■	3	▪	▪	■	1	■
■	■	■	■	■	■	■
2	▪	■	1	■	▪	▪
■	■	■	■	■	■	▪
■	1	■	▪	2	■	▪
■	■	2	■	■	■	▪
1	■	▪	■	1	■	6

Try it yourself

`https://www.brainbashers.com/nurikabe.asp`

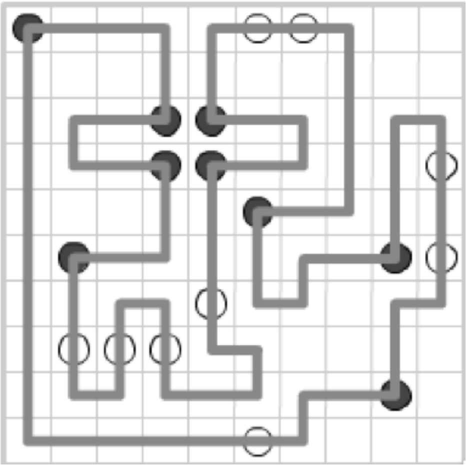
Puzzle 4: Masyu



●		○			○	○			
			○					○	○
●		●	○			○			
			●		●	○			
○	○	○			●		○	●	
						●		●	
	●			○					○
					●	○			
	○	○	○		○	●	○	○	
						○			

What are the rules of this game?

Puzzle 4: Masyu continued



Try it yourself

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