Advanced Cryptography

Chapter #0: Introduction

Serge Vaudenay

EPFL

https://lasec.epfl.ch/

COM-501 Advanced Cryptography 2025: v4.7

- continuation of *COM-401 Cryptography and Security*
  WARNING: this course is much harder!
- cryptanalysis: weaknesses in some cryptographic schemes
- security proof techniques for cryptographic schemes
- foundations
- more cryptographic schemes: interactive proof

Chapters

1. **The Cryptographic Zoo**
   reminders, prerequisites
2. **Cryptographic Security Models**
   definitions and security formalisms, games, proofs
3. **Cryptanalysis (Public-Key)**
   implementation issues, famous failure cases
4. **The Power of Interaction**
   interactive proofs and zero-knowledge
5. **Cryptanalysis (Conventional)**
   statistical analysis
6. **Proving Security**
   random oracles, hybrid cryptography

Prerequisites

- **CS-250 Algorithms**, BSc
- **CS-251 Theory of Computation**, BSc
- **MATH-310 Algebra**, BSc
- **COM-401 Cryptography and Security**, MSc
  WARNING: *COM-501* may be hard to follow if you did not fully master *COM-401*

Some Useful Backgound

- algorithmics
- probability theory (discrete)
- discrete math (combinatorics, graphs, etc)
- algebra (group theory, finite fields)
- number theory (arithmetics)
- complexity theory (problem reduction)

Material

- these slides and other information on the web site

  `https://moodle.epfl.ch/course/view.php?id=13913`

- on the web: previous exams (with solutions)

  `https://lasec.epfl.ch/courses/exams_archives.php`

- on the web: online survey trainer

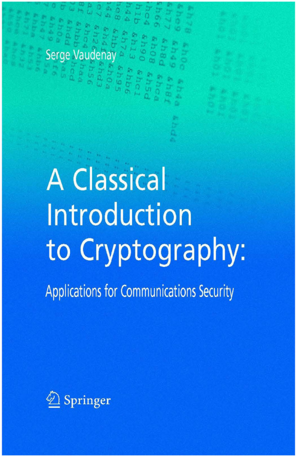
  `https://lasec.epfl.ch/quizgen/quiz.html`

- Springer lecture notes (made for v2!)

  `https://www.vaudenay.ch/crypto/`

- lecture notes + videos (from 2021)

A Classical Introduction to Cryptography

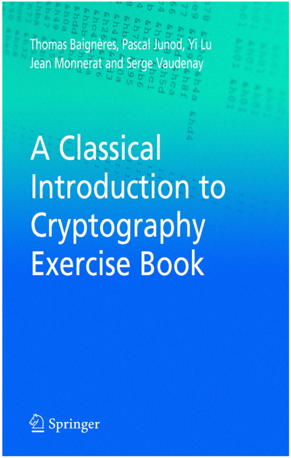


Serge Vaudenay

A Classical Introduction to Cryptography:

Applications for Communications Security

Springer



Thomas Baignères, Pascal Junod, Yi Lu
Jean Monnerat and Serge Vaudenay

A Classical Introduction to Cryptography Exercise Book

Springer

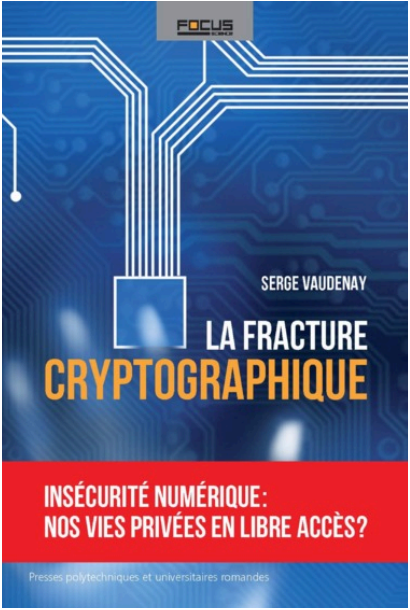
textbook

exercise book

`https://www.vaudenay.ch/crypto/`

Warning: adapted to v1–v2 only

La Fracture Cryptographique


FOCUS SCIENCE
SERGE VAUDENAY
LA FRACTURE
CRYPTOGRAPHIQUE
INSÉCURITÉ NUMÉRIQUE:
NOS VIES PRIVÉES EN LIBRE ACCÈS?
Presses polytechniques et universitaires romandes

Further References

1. **Stinson**. *Cryptography, Theory and Practice (3rd Edition).* CRC. 2005.
   Good lecture notes
2. **Menezes-van Oorschot-Vanstone**. *Handbook of Applied Cryptography.* CRC. 1997.
   `https://cacr.uwaterloo.ca/hac/`
   Reference book (not to be read from a to z)
3. **Shoup**. *A Computational Introduction to Number Theory and Algebra.* Cambridge University Press. 2005.
   `https://shoup.net/ntb`
   Textbook on algebra for cryptographers and applications.
4. **Joux**. *Algorithmic Cryptanalysis.* CRC. 2009.

Schedule and Policy (2025)

prerequisites: *Cryptography and Security*

lectures: Thursday 10.15–12.00

midterm exam: 17.4 (105min open books)

survey: when announced (closed books)

homeworks: when announced

$$\begin{aligned}
\text{grade} &= \operatorname*{bound}_{[\text{exam}-1,\text{exam}+1]} \frac{\text{exam} + \text{continuous}}{2} \\
\text{continuous} &= 0.4 \times \text{midterm} + 0.3 \times \text{surveys} + 0.3 \times \text{homeworks} \\
\text{surveys} &= \text{average}\,(\text{best surveys}) \qquad \text{2 out of 4} \\
\text{homework} &= \text{average}\,(\text{homework}) \qquad 2
\end{aligned}$$

Surveys

- 10 minutes during the course (announced one week before)
- 5 multiple choice questions (4 choices per question)
- one and only one answer correct
- an extra bonus question
- grading system

$$\text{grade}=\text{bound}_{[1,6]}\left(1+\#\text{good answers}-\frac{\#\text{bad answers}}{2}+\text{bonus}\right)$$

  pretty harsh

- **better no answer than a bad one!**

Homeworks

1. analysis/experiment
2. implementing algorithms
3. writing math proof

IT WILL BE TOUGH!

Grade Statistics — Advanced Cryptography

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
# students at exam	3	8	9	20	8	9	10	5	11	15	18	16	8	12	16	19	23	24	15	23
success rate	100%	88%	89%	75%	75%	89%	100%	100%	91%	93%	88%	100%	62%	75%	100%	100%	95%	87%	93%	86%
average grade	4.67	4.75	5.11	4.30	4.19	4.50	4.75	5.10	5.05	4.90	4.75	4.88	4.16	4.40	4.75	5.34	5.04	4.95	4.97	4.65
6.00		3	3		3	2	2	2	4	4	3	1		1		5	1	1	2	2
5.75														1		3	5	2	1	
5.50			2	2					2	3	4	4		1	3	2	1	6		2
5.25													1		2	2	4	3	2	1
5.00	2		1	4		1	3	1	2	2	1	5	1	1	2	3	6	3	4	4
4.75													1	2	2	1	3	1	2	3
4.50		2	2	5	1	1	1	1		2	7	2		1	3	1	1	3	2	3
4.25																2		2		2
4.00	1	2		4	2	4	4	1	2	3	1	4	2	2	4		1		1	3
3.75													1	1				1	1	1
3.50				3							0		1					2		1
3.25																				1
3.00		1	1	2		1					1		1							
2.75														1						
2.50									1											
2.25																				
2.00										1	1			1			1			
1.75																				
1.50					2															
1.25																				
1.00																				

Q & A