Cryptography and Security

Advanced Cryptography

Serge Vaudenay

EPFL

`http://lasec.epfl.ch/`

Advanced Cryptography 2021: v4.3

- continuation of *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

- **Cryptography and Security**, MSc
  ...and all its prerequisites
  WARNING: *Advanced Cryptography* may be hard to follow if you did not fully master *Cryptography & Security*
- *Informatique théorique*, BSc

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

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

- on the web: previous exams (with solutions)

  `http://lasec.epfl.ch/courses/exams_archives.shtml`

- on the web: online survey trainer

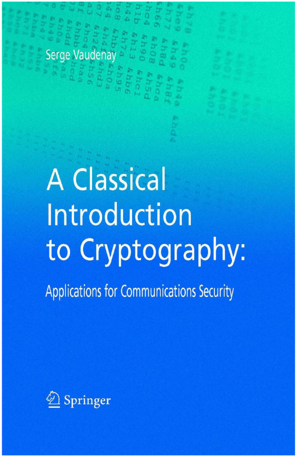
  `http://lasec.epfl.ch/quiz_generator/choices.php`

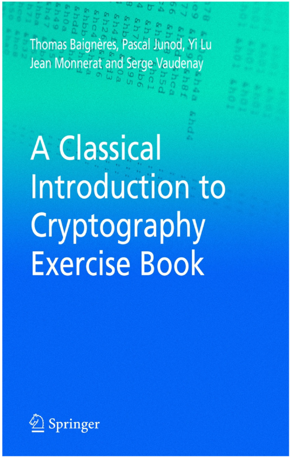
- Springer lecture notes (made for v2!)

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

- lecture notes

A Classical Introduction to Cryptography


Serge Vaudenay
A Classical Introduction to Cryptography:
Applications for Communications Security
Springer

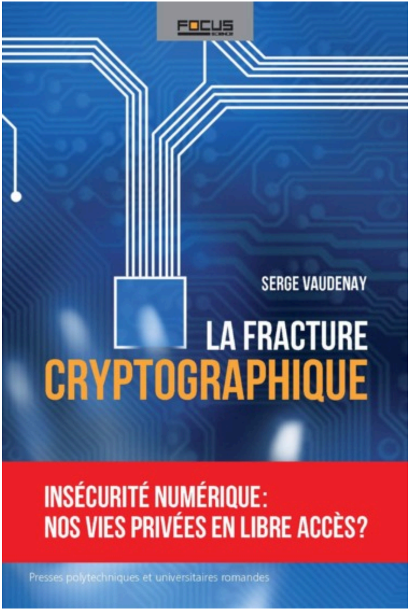

Thomas Baignères, Pascal Junod, Yi Lu
Jean Monnerat and Serge Vaudenay
A Classical Introduction to Cryptography Exercise Book
Springer

textbook exercise book

`http://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.
   `http://www.cacr.math.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.
   `http://shoup.net/ntb`
   Textbook on algebra for cryptographers and applications.
4. **Joux**. *Algorithmic Cryptanalysis.* CRC. 2009.

Schedule and Policy (2021)

prerequisites: *Cryptography and Security*

lectures: 25.2 - 4.3 - 11.3 - 18.3 - 25.3 - 1.4 - 15.4 - 22.4 - 29.4 - 6.5 - 20.5 - 27.5 - 3.6

midterm exam: 29.4 (180min open books)

survey: when announced (closed books)

homeworks: when announced

$$
\begin{aligned}
\text{grade} &= \underset{[\text{exam}-1,\text{exam}+1]}{\text{bound}} \frac{\text{exam}+\text{continuous}}{2} \\
\text{continuous} &= 0.4\times\text{midterm}+0.3\times\text{surveys}+0.3\times\text{homeworks} \\
\text{surveys} &= \text{average}\,(\text{best surveys}) \qquad \text{2 out of 4} \\
\text{homework} &= \text{average}\,(\text{best homework}) \qquad \text{2 out of 3}
\end{aligned}
$$

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
# students at exam	3	8	9	20	8	9	10	5	11	15	18	16	8	12	16	19
success rate	100%	88%	89%	75%	75%	89%	100%	100%	91%	93%	88%	100%	62%	75%	100%	100%
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
6.00		3	3		3	2	2	2	4	4	3	1		1		5
5.75														1		3
5.50			2	2					2	3	4	4		1	3	2
5.25													1		2	2
5.00	2		1	4		1	3	1	2	2	1	5	1	1	2	3
4.75													1	2	2	1
4.50		2	2	5	1	1	1	1		2	7	2		1	3	1
4.25																2
4.00	1	2		4	2	4	4	1	2	3	1	4	2	2	4	
3.75													1	1		
3.50				3							0		1			
3.25																
3.00		1	1	2		1					1		1			
2.75														1		
2.50									1							
2.25																
2.00										1	1			1		
1.75																
1.50					2											
1.25																
1.00																

Q & A