

Cryptography and Security

Chapter #0: Introduction

Serge Vaudenay



<http://lasec.epfl.ch/>

LASEC

DIVERSITY IS
OUR STRENGTH



EPFL

Chapter 0: Preamble



Chapter 0: Preamble

- Information About the Course
- Other Courses

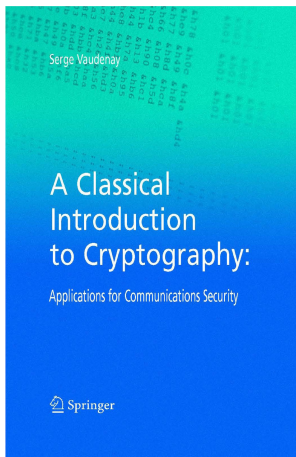
Learning Goals

- sense of adversarial thinking
- model security problems in terms of games
- math background for public key crypto
- wide overview on the crypto domain
- key length choices

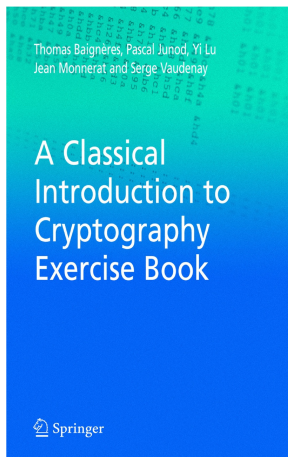
COM-401 Cryptography & Security 2024: v4.12

- This lecture has been given since 1999–2000.
- v1: complete lecture on cryptography
- v2: split basic/advanced, basic merged with network security
lecture notes for v2 by Springer
- v3 (2008–13): less analysis, more examples
- v4 (since 2013–14): major revision
new structure: more integrated chapters

A Classical Introduction to Cryptography



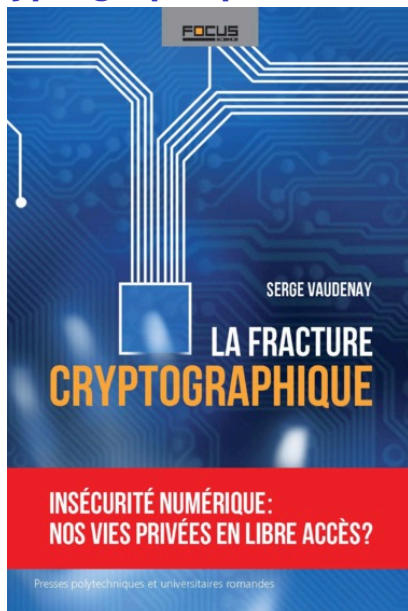
textbook



exercise book

<http://www.vaudenay.ch/crypto/>

La Fracture Cryptographique



Content of this Lecture

1 Ancient Cryptography:

Vigenère, Enigma, Shannon theory

2 Diffie-Hellman Cryptography:

algebra, Diffie-Hellman, ElGamal

3 RSA Cryptography:

number theory, RSA, factoring

4 Elliptic Curve Cryptography:

elliptic curves over a finite field, ECDH, ECIES, pairing

5 Symmetric Encryption:

block ciphers, stream ciphers, exhaustive search

6 Integrity and Authentication:

hashing, MAC, birthday paradox

7 Public-Key Cryptography:

cryptosystem, signature, pq-crypto

8 Trust Establishment:

pwd-based crypto, secure communication, trust setups

++ Case Studies:

WiFi, Bitcoin, mobile telephony,

WhatsApp, EMV, Bluetooth,

biometric passport, TLS

Material

- these slides

<http://moodle.epfl.ch/course/view.php?id=13671>

- on the web: previous exams (with solutions)

http://lasec.epfl.ch/courses/exams_archives.php

- on the web: online survey trainer

<http://lasec.epfl.ch/quizgen/quiz.html>

- Springer lecture notes (v2)

<http://www.vaudenay.ch/crypto/>

- lecture notes (can be incomplete)
- videos (from 2020 and 2021)
- executive summary

WARNING: slides are made for students attending the course:
don't even hope you can catch up by just reading the slides!

Provided Material

- presences in class is not mandatory (but recommended)
material (slides, old video) is provided to help to catch up
- some old exercise solutions may be laconic
do not hesitate to ask for help (TAs, forum, me)

Other References

- ❶ **Stinson.** *Cryptography, Theory and Practice (3rd Edition)*. CRC. 2005.
Good lecture notes
- ❷ **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)
- ❸ **Shoup.** *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press. 2005.
<http://shoup.net/ntb>
Textbook on algebra for cryptographers and applications.

WARNING

- lots of math in this course, including PROBABILITIES
HOWEVER: it is not the purpose to teach math and proba
we give “reminders”
exercises/exams may be based on it
- mostly theory
+ a few case studies
- many topics superficially covered
→ more in Advanced Cryptography

think twice before registering to this course!

Relevant BSc Courses

mandatory:

- MATH-310 **Algebra**
- MATH 232 **Probabilities and statistics**
- CS-250 **Algorithms**

recommended:

- COM-301 **Computer security**

Prerequisites Test

- will happen on week 2 during the exercise session
- optional
- reward: grade of 4.0 or more gives a 0.5 bonus to the homework grade
- (not counted otherwise)

Schedule and Grading

lectures: Wednesday 8.15-10.00 and Thursday 10.15-12.00

exercises: Friday 9.15-11.00

midterm exam: 30.10 (closed books)

survey: about once per chapter (closed books)

$$\begin{aligned} \text{grade} &= \arg \min_{x \in [\text{exam}-1, \text{exam}+1]} \left| x - \frac{\text{exam} + \text{continuous}}{2} \right| \\ \text{continuous} &= \text{sum}(0.4 \times \text{midterm}, 0.3 \times \text{surveys}, 0.3 \times \text{homework}) \\ \text{surveys} &= \text{average}(\text{best surveys}) && 3 \text{ out of } 5 \\ \text{homework} &= \text{average}(\text{homework}) + \text{bonus}(\text{prereq}) && 2 \end{aligned}$$

What is this Crazy Grade Formula?

$$\text{grade} = \arg \min_{x \in [\text{exam} - 1, \text{exam} + 1]} \left| x - \frac{\text{exam} + \text{continuous}}{2} \right|$$

= grade from the $[\text{exam} - 1, \text{exam} + 1]$ interval which is the closest to $\frac{\text{exam} + \text{continuous}}{2}$

- if $\frac{\text{exam} + \text{continuous}}{2}$ is in the interval, this is the final grade
- if $\frac{\text{exam} + \text{continuous}}{2} > \text{exam} + 1$, the final grade is $\text{exam} + 1$
- if $\frac{\text{exam} + \text{continuous}}{2} < \text{exam} - 1$, the final grade is $\text{exam} - 1$

Your Personal Work

- attend to the lecture and **take notes!**
- understand the lectures, prepare for surveys
(tip: pay special attention to slides with a red title!)
no need to learn algorithms by heart
- work on exercises given in the exercise sessions
- do your homework
- work by yourself on past exams
- **ask questions**
- **ask us for help if you need it**

course has 8 ECTS credits:

on average, students must work > 10 h per week on this course

(including 3h of courses and 1.5h of exercises)

Surveys

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

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

- **better no answer than a bad one!**
yes, this is harsh!
- objective:
check that a chapter is understood
maintain the pressure!

Homework

- in group of 2
- solving/implementing/computing exercises in **sage**
(introduction on sage to come)
- proving

Exams

Midterm and Final Exams

- written exam with limited time
- no device such as computer, smartphone, tablet allowed
- pocket calculator allowed (and sometimes useful)
- no documents allowed (except what follows)
- 2-sided sheet of hand-written notes allowed (both exams)
- handwritten with fill-in-box forms
- look at previous exams!

How are Exams Graded

- grades are scaled based on what expected proportion of the solutions qualifies for a 4.0
- some students may exceed our expectations, ...but grades go up to 6.0 only 😊
- we do not expect students to cover all questions

we don't give the exact grading scales but all questions have the same weight

Grade Statistics — (v1) Cryptography and Security

	2001	2002	2003	2004
# students at exam	14	58	56	84
success rate	100%	90%	63%	75%
average grade	4.64	4.40	4.00	4.07
6.0	1			2
5.5	1	2	5	6
5.0	3	13	7	9
4.5	5	21	10	18
4.0	4	16	13	28
3.5		5	13	9
3.0		1	7	5
2.5				2
2.0			1	1
1.5				3
1.0				1

Grade Statistics — (v2) Cryptography and Security

	2004–05	2005–06	2006–07	2007–08
# students at exam	90	127	110	106
success rate	48%	90%	74%	85%
average grade	3.60	4.55	4.20	4.47
6.0	4	4	2	2
5.5	4	14	10	12
5.0	15	34	17	26
4.5	12	36	23	29
4.0	8	26	29	21
3.5	12	8	17	8
3.0	10	3	4	7
2.5	7	1	6	1
2.0	6	1	1	
1.5	7		1	
1.0	5			

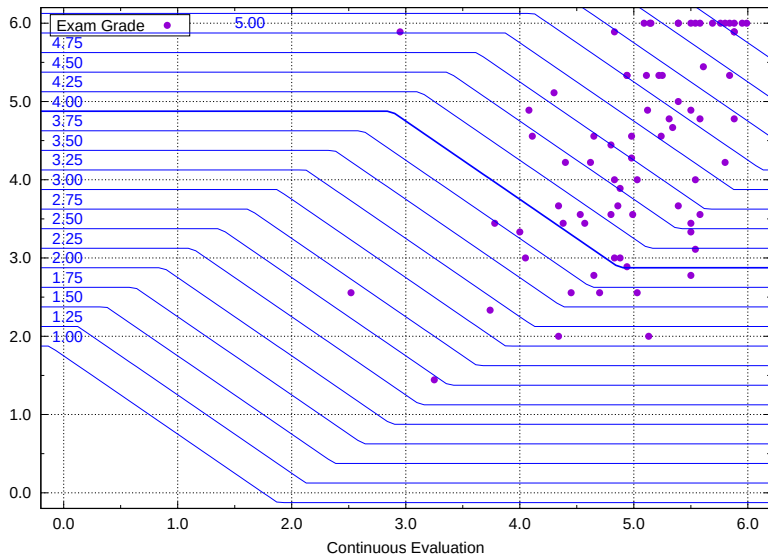
Grade Statistics — (v3) Cryptography and Security

	2008–09	2009–10	2010–11	2011–12	2012–13
# students at exam	72	41	109	107	65
success rate	81%	95%	77%	65%	72%
average grade	4.34	4.76	4.38	4.07	4.21
6.0	4	5	6	4	5
5.5	9	6	15	10	2
5.0	12	8	18	11	9
4.5	12	11	31	18	15
4.0	21	9	14	27	16
3.5	4	1	11	17	8
3.0	6	1	6	9	7
2.5	2		2	8	2
2.0	2		5	3	1
1.5			1		
1.0					

Grade Statistics — (v4) Cryptography and Security

	2013–14	2014–15	2015–16	2016–17	2017–18	2018–19	2019–20	2020–21	2021–22	2022–23	2023–24
# students at exam	76	90	109	86	47	72	60	66	89	87	76
success rate	96%	95%	88%	87%	85%	90%	88%	90%	79%	75%	82%
average grade	4.87	4.84	4.64	4.50	4.79	4.80	4.84	5.00	4.76	4.49	4.69
6.00	9	9	14	1	4	4	7	6	4	3	8
5.75				3	2	8	6	10	6	4	6
5.50	16	15	19	4	4	7	7	14	6	9	5
5.25				9	8	8	4	8	9	7	10
5.00	18	28	29	8	7	6	6	5	15	8	6
4.75				9	4	9	7	2	14	8	4
4.50	19	23	25	19	3	11	8	8	11	7	10
4.25				7	3	4	3	4	8	12	6
4.00	11	11	17	15	5	8	5	3	6	8	8
3.75				3	5	2	3		7	10	3
3.50	1	3	4	4	1	2		3	1	1	5
3.25				1		1	2	1		3	
3.00	1			1	1	1	1		2	3	3
2.75				1						3	
2.50			6			1		1		1	1
2.25				1							1
2.00	1		1					1			
1.75							1				
1.50		1	2								
1.25											
1.00			1								

Continuous Work is Really Important!



Feedback are Valuable

- if there is something you did not understand
→ please ask questions
- if you are lost
→ please stop me
- if you see errors or have remarks to improve the slides
→ please let me know
- if you have suggestion of any kind
→ please let me know

it is counterproductive to wait until the course evaluation to give feedback!



Chapter 0: Preamble

- Information About the Course
- Other Courses

Specialization in ~~Information Security~~ Cyber Security - SP

course title	volume	credits	lecturer
COM-401 Cryptography and Security	56+28	8	Vaudenay
COM-402 Information Security and Privacy	42+42	8	Payer
COM-405 Mobile Networks	42+28	8	Al Hassanieh
COM-407 TCP/IP Networking	28+56	8	Nikolopoulos
COM-417 Algorithms II	56+42	8	Kapralov, Svensson
CS-459 Foundations of Probabilistic Proofs	56+14	6	Chiesa
CS-477 Advanced Operating Systems	28+42	6	Kashyap
CS-510 Topics in Software Security	14+14	3	Payer
CS-522 Principles of Computer Systems	56+0	8	Argyaki, Candea
CS-550 Formal Verification	28+56	6	Kuncak
CS-412 Software Security	42+42	6	Payer
CS-470 Advanced Computer Architecture	42+28	8	Ienne
MATH-489 Number Theory II.c - Cryptography	28+28	5	Jetchev
COM-501 Advanced Cryptography	28+28	6	Vaudenay
COM-506 Student Seminar: Security Protocols and Applications	0+28	3	Vaudenay
CS-523 Advanced Topics on Privacy Enhancing Technologies	42+42	8	Troncoso

Kudelski Award

2005	Martin Vuagnoux AUTODAFE: an Act of Software Torture
2006	Sylvain Pasini Secure Communications over Insecure Channels Using an Authenticated Channel
2007	Alexandre Karlov Broadcast Encryption and Traitor Tracing using Elliptic Curves
2009	Benoît Dupasquier Encrypted VoIP Speech Recognition
2010	Thomas Hofer Evaluating Static Source Code Analysis Tools
2011	Alexandre Duc Unaligned Rebound Attack: Application to Keccak
2014	Sylvain Heiniger TPROXY: A Versatile Interception Proxy
	Benjamin Wesolowski Walking on Isogeny Graphs of Genus 2 Hyperelliptic Curves
2015	Paul Bottinelli Computational Aspects of Correlation Power Analysis Attacks
2017	Thomas Mizraji Extracting Cyber Threat Intelligence from the Internet Background Noise
2020	Arnaud Pannatier A Control Plane in Time and Space for Locality-Preserving Blockchains
2021	Mathilde Raynal Secure Implementation and Performance Evaluation of Post-Quantum Cryptography
2022	Bastien Wermeille AppSec Lifecycle Assessment
2023	Antoine Sidem Tapping Electromagnetic Emanations of Smartphones
2024	??

Semester Project / Master Thesis

- list of available proposals at LASEC:
<http://lasec.epfl.ch/teaching.php>
- bring your own ideas

Student Seminar: Security Protocols and Applications

Serge Vaudenay

- (team of) students give courses on negotiated topics
- written lecture notes (by the students)
- also graded by peers!
- best lectures serve as topics for the final exam

Grade Statistics — Student Seminar: SPA

	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
# students at exam	10	12	28	13	13	9	13	9	9	11	13	25	15	15	9	9	11	17	26	12	21
success rate	100%	92%	96%	100%	100%	100%	92%	100%	100%	91%	92%	100%	93%	100%	100%	100%	100%	100%	100%	91%	100%
average grade	5.45	4.58	4.73	5.23	5.15	5.39	5.08	5.06	5.44	4.86	4.73	5.28	5.60	5.08	5.56	5.19	5.34	5.54	5.74	5.25	5.92
6.00	2	1		1		3	2		1	1			9	2	5	1	1		13	2	18
5.75														1	1	1	2	5	6	5	2
5.50	6	1	6	7	6	3	4	4	6	3	5	15	4	2	3	1	3	10	2		
5.25														3		2	1	2	4		
5.00	1	4	8	3	6	1	3	2	2	3	1	9	1		1	3			1	3	1
4.75														4							
4.50	1	1	8	1		2	2	3		2	3	1		1	1				1	1	
4.25														1	1						
4.00		4	5	1	1		1			1	3			1		1					
3.75																				1	
3.50							1				1										
3.25																					
3.00		1								1			1								
2.75																					
2.50																					
2.25																					
2.00																					
1.75																					
1.50																					
1.25																					
1.00																					

Advanced Cryptography

Serge Vaudenay

The follow up (advanced part) of this course since v3:

- more protocols: zero-knowledge, secret sharing
- cryptanalysis methods
- security analysis
- provable security

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															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																1		2		2
4.00	1	2		4	2	4	4	1	2	3	1	4	2	2	4	2	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							1
2.75														1						
2.50									1											
2.25										1	1				1					
2.00																	1			
1.75																				
1.50					2															
1.25																				
1.00																				



- Excuse me, is this the Service for asking stupid questions?