

MAP-i
Programa Doutoral em Informática
Mathematical Foundations of Cryptology
Unidade Curricular em Teoria e Fundamentos
(UCTF)
Universidade do Porto

May 9, 2011

Abstract

This document describes a Ph.D. level course Mathematical Foundations of Cryptology UCTF (“Unidade Curricular em Teorias e Fundamentos”) of the PhD program MAP-i, corresponding to a Curriculum Unit credited with 5 ECTS. The course provides a standard introduction to the Number Theory and Algebra required to understand most of the contemporary cryptographic algorithms as well as a comprehensive introduction to the current and past main trends in Cryptography and its applications.

Lecturing Team

Universidade do Porto

- António Machiavelo (Dep. Matemática da Faculdade de Ciências)
- Rogério Reis (Dep. Ciência dos Computadores da Faculdade de Ciências)

Universidade do Minho

- José Assis Azevedo (Departamento de Matemática e Aplicações)
- José Pedro Patrício (Departamento de Matemática e Aplicações)

1 Introduction

The crucial role of security in communication networks and computer systems makes vital the necessity of educating persons that are knowledgeable of modern

cryptographic developments. Today several cryptographical protocols are essential in electronic transactions and businesses. Digital signatures, key distribution protocols, integrity and authenticity of information, as well as confidentiality, are all dependent on cryptography.

With this unit we intend to provide a solid introduction to cryptography and its mathematical background. It presents the concepts and fundamental results of Number Theory and Algebra that form the backbone of contemporary cryptography. Equipped with this, students can then grasp the ideas behind modern cryptosystems, as well as to understand all the details of their inner workings.

ACM Computing Classification System subjects covered:

- E. Data (E.3 DATA ENCRYPTION, E.4 CODING AND INFORMATION THEORY (H.1.1))
- F. Theory of Computation (F.2 ANALYSIS OF ALGORITHMS AND PROBLEM COMPLEXITY (B.6, B.7, F.1.3))
- G. Mathematics of Computing (G.2 DISCRETE MATHEMATICS, G.3 PROBABILITY AND STATISTICS)

2 Objectives

The main goal of this course is to provide students with a solid knowledge of the mathematical background without which one cannot understand modern cryptography and its protocols. This will allow to present in great detail the major modern cryptosystems, without any recourse to “black boxes”. We believe that this is the only way to equip students with the necessary tools to have a deep understanding of current systems and protocols, to follow recent and future developments, and eventually to participate in some of those developments. Moreover, this mathematical tools can only be fully assimilated if the students have the opportunity to operationalize them in a sound and powerful environment like the one provided by SAGE (<http://www.sagemath.org>), an open source computer algebra system, built out of 95 open-source packages underneath a unified interface¹ Its programming language is the world-wide known Python. Sage has been used not only for educational purposes, but for research as well. The list of publications presented at <http://www.sagemath.org/library-publications.html> shows Sage’s impact in the scientific community. The references [Ste09] and [Was03] show how Sage can be used as a scientific tool in cryptography.

¹A comprehensive list of these packages is available at <http://www.sagemath.org/links-components.html>.

3 Teaching Goals

The students should be able to:

- choose the appropriate protocol to use either at the user, programmer or system administrator level;
- analyze, modify, choose and write the necessary protocol for any concrete application;
- study the possibility of cryptanalytic attacks to new protocols;
- read and have a critical judgement about a cryptographical product description or on a scientific working paper on the subject.

4 Course contents

1. Brief introduction to SAGE and some of its tools, to be used throughout the course.
2. Classical Cryptography and Cryptanalysis
 - Monoalphabetic ciphers and their weaknesses
 - Polyalphabetic ciphers and their statistical cryptanalysis
 - Some esoteric ciphers and their cryptanalysis
 - Some electromechanical ciphers and their cryptanalysis
3. Brief notions of Cryptography
 - Cryptographic hash functions
 - One-way functions and one-way functions with trapdoor
 - Symmetric criptography vs public key cryptography
 - Cryptographical pseudo random number generators
4. Number Theory
 - Euclidean Algorithm and the Fundamental Theorem of Arithmetic
 - Congruences, Fermat's "little" theorem, and Euler's totient theorem.
 - The RSA and Paillier cryptosystems
 - Chinese Remainder Theorem
 - Quadratic residues, Legendre and Jacobi symbols, and quadratic reciprocity
 - Fast arithmetic algorithms for long integers
5. Algebra

- Basic results on groups, rings and fields
 - Review of basic linear algebra, including Gaussian elimination method
 - Polynomial rings and their quotients
 - Finite fields and their classification
 - The Rijndael (AES) cipher
 - The Diffie-Hellman key-generation, ElGamal and Rabin-Williams ciphers
6. Prime numbers and factoring
- Eratosthenes sieve and naive primality tests.
 - Probabilistic primality tests
 - The AKS primality test
 - Fermat factoring method
 - The quadratic sieve
 - The number field sieve
7. Elliptic Curves
- Elliptic curves and their arithmetic
 - Elliptic curves over finite fields
 - Elliptic curve cryptography
8. Cryptographical Protocols
- Some elementary cryptographic protocols, for authentication and signature.
 - Sophisticated protocols for voting, e-money, time-stamping, and other protocols allowing the migration to the web of complex social interactions.

5 Teaching Methods

- Lectures and invited lectures.
- Occasional tool demonstrations.

6 Student Assessment

- Examinations.
- Assignments, which may include an oral presentation by the student.

References

- [Bar09] Gregory V. Bard. *Algebraic Cryptanalysis*. Springer, 2009.
- [Bau97] F. L. Bauer. *Decrypted Secrets. Methods and Maxims of Cryptology*. Springer, 1997.
- [CP01] Richard Crandall and Carl Pomerance. *Prime Numbers. A Computational Perspective*. Springer, 2001.
- [Gai39] Helen Fouché Gaines. *Cryptanalysis. A study of ciphers and their resolution*. Dover Publications, 1939.
- [HPS08] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.
- [Kah67] David Kahn. *The Codebreakers. The Story of Secret Writing*. Scribner, 1967.
- [Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993.
- [Kob94] Neal Koblitz. *A course in Number Theory and Cryptography*. Number 114 in Graduate Texts in Mathematics. Springer, second edition, 1994.
- [LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. CUP, second edition, 1997.
- [MvOV96] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- [Sch96] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, Inc, second edition, 1996.
- [Sho08] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.
- [Ste09] William Stein. *Elementary Number Theory: Primes, Congruences, and Secrets*. Springer, 2009.
- [Vin77] I. Vinogradov. *Fundamentos de la Teoria de los Numeros*. MIR, 1977.
- [Was03] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, 2003.