Cryptography and Information Security
MAP-I Curricular Unit – 2010/2011

Summary

This document describes a Ph.D. level course, corresponding to a Curriculum Unit credited with 5 ECTS. It is offered jointly by the CCTC/Departamento de Informática at Universidade do Minho and IT/Departamento de Ciência de Computadores at Faculdade de Ciências da Universidade do Porto in the MAP-I doctoral program.

The objective of this course is to introduce students to the theoretical principles that underly current research in modern cryptography. The focus is on a rigorous *approach to information security, emphasizing the central role of definitions and formal proofs of security, resorting to simple and precisely stated assumptions.*

Coordinator: Manuel Barbosa (CCTC/DI-UM)

Context

This document describes a Ph.D. level course, corresponding to a Curriculum Unit credited with 5 ECTS. It is offered jointly by the CCTC/Departamento de Informática at Universidade do Minho and IT/Departamento de Ciência de Computadores at Faculdade de Ciências da Universidade do Porto in the MAP-I doctoral program.

This proposal aims to instantiate the Curricular Unit in Theory and Foundations of Computer Science or, alternatively, the Curricular Unit in Technologies.

This proposal is a spin-off version of the *Advanced Topics in Information Security* (ATIS), which was accepted in all previous editions of the MAP-I doctoral program under the Foundations of Computing topic, and accredited by Carnegie Mellon University within the CMU-Portugal initiative. With respect to the ATIS syllabus, the proposed course focuses on the theoretical aspects of modern cryptography, leaving out the more technological aspects.

The course is offered exceptionally for the 2010/2011 edition of the MAP-i doctoral programme.

Course Description

The objective of this course is to introduce students to the theoretical principles that underly current research in modern cryptography and information security. The focus is on a *rigorous* approach to information security, emphasizing the

central role of definitions and formal proofs of security, resorting to simple and precisely stated assumptions.

Prerequisites

Students are expected to have an undergraduate background in Computer Science. In particular, familiarity with basic discrete mathematics and the concept of a mathematical proof is important, as well as background knowledge on algorithms. Prior knowledge of cryptography and complexity theory are desirable, but not necessary. Students who have not previously taken courses in these topics may have to work harder and do more outside reading in order to keep up.

Textbooks and Other Required Materials

The course is at a similar level and covers overlapping material with the following advanced modules taught at leading academic institutions in the information security area, namely:

- Modern Cryptography, Mihir Bellare, UCSD.
- Introduction to Cryptography, Yevgeniy Dodis, NYU.
- Introduction to Cryptography, D. Boneh, Stanford.

Recommended reading materials include:

- Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC.
- Foundations of cryptography Vol. 1 and 2, Oded Goldreich, Cambridge University Press.
- Lecture Notes on Cryptography, M. Bellare and S. Goldwasser (available on-line)
- Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway (available on-line)
- A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press
- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Ooorschot, and S.A. Vanstone (available on-line)

Course Objective

The course will cover theoretical issues in cryptography with important applications in information security, and students are expected to acquire the following skills:

- Familiarity with scientific challenges in cryptography and information security.
- Ability to extract information from scientific papers in the area.
- Technical writing and presentation skills.
- Comfortability with security proofs and ability to think abstractly about information security problems.

Topics Covered

1. Introduction: Basic Principles of Modern Cryptography, Perfectly-Secret Encryption, One-Time Pad, Limitations of Perfect Secrecy.
2. Symmetric Cryptography: Computationally-Secure Encryption, Stream Ciphers and Multiple Encryptions, Permutations and Block Ciphers, Modes of Operation, Practical Constructions of Pseudorandom Permutations, Message Authentication Codes, MAC Constructions, Cryptographic Hash Functions.
3. Constructions of Pseudorandom Objects: One-Way Functions, Hard-Core Predicates, Pseudorandom Generators, Pseudorandom Functions, Computational Indistinguishability.
4. Number Theory and Cryptographic Hardness Assumptions: Algebraic Background, Factoring Assumption, RSA Assumption, Discrete Logarithm and Diffie-Hellman Assumptions, Introduction to Elliptic Curves, Bilinear Pairings and Related Computational Assumptions.
5. Public-Key Cryptography: Security against Chosen-Plaintext Attacks, Hybrid Encryption, RSA and ElGamal, Security Against Chosen-Ciphertext Attacks, Digital Signatures, RSA Signatures, "Hash-and-Sign" Paradigm, One-Time Signatures, Public-Key Cryptosystems in the Random Oracle Model.
6. Identity Based Cryptography: Concept, Identity Based Signatures and Encryption, Concrete Schemes in The Random Oracle Model, Chosen Ciphertext Secure Public-Key Encryption from Identity Based Encryption.
7. Zero Knowledge Proofs, Proofs of Knowledge and Non-Interactive Zero Knowledge Proofs.

Expected Number of Students

Expected number of students is 15.

Class Schedule

Lectures, discussions and student presentations. The course corresponds to 42 lecturing hours, during one complete semester. Tentative class schedule: 2 hour lecture + 1 hour tutorial per week, for 14 weeks.

Student Evaluation Criteria

- 50% Final exam
- 40% Written assignments and paper presentations
- 10% Class participation

A total final score under 50% means the student fails the course and must re-take a final exam which will then represent 100% of the final score.

Course Staff

Teaching workload will be evenly distributed among the following instructors:

- Manuel B. Barbosa (DI-UM) – Contact person (`mbb@di.uminho.pt`)
- José M. Valença (DI-UM)
- Luis Antunes (IT/DCC-FCUP)