School of Informatics Teaching Course Proposal Form

This version was generated **March 2, 2016**. User 'akiayias@inf.ed.ac.uk' verified.

Proposal

Course Name: Cryptography
Proposer's Name: Aggelos Kiayias
Email Address: akiayias@inf.ed.ac.uk
Course Year: 4
Names of any courses that this new course replaces :
none

Course Outline

Course Level: 11
Course Points: 10
Subject area: Informatics
Programme Collections:
Computer Science.

Teaching / Assessment

Number of Lectures: 20
Number of Tutorials or Lab Sessions: 0
Identified Pre-requisite Courses: Recommended (INFR10058) AND (INFR09006) OR (INFR10052)
Identified Co-requisite Courses: none
Identified Prohibited Combinations: none

Assessment Weightings:
Written Examination: 90%
Assessed Coursework: 10%
Oral Presentations: 0%

Description of Nature of Assessment:
There will be a homework counting for 10% of the final grade related to the objectives 1-2.

Course Details

Brief Course Description:
Cryptography is the formal study of the notion of security in information systems. The discipline focuses on various problems pertaining to secure communication and computation. It entails the study of models that express security properties as well as the algorithms and protocols that are the implementation candidates for satisfying these properties. An important dimension of modern cryptography is the design of security proofs that establish security properties. Such proofs are conditional on assumptions that fall in two categories: "system assumptions" such as the faithful execution of code, or the availability of private randomness and "computational assumptions" that are related to the computational complexity of various problems (including factoring large numbers and others).

The course will offer a thorough introduction to modern cryptography focusing on models and proofs of security for various basic cryptographic primitives and protocols including key exchange protocols, commitment schemes, digital signature algorithms, oblivious transfer protocols and public-key encryption schemes. Applications to various problems in secure computer and information systems will be briefly discussed including secure multiparty computation, digital content distribution, e-voting systems, digital payment systems, cryptocurrencies.

Detailed list of Learning Objectives:

1. Understand basic group theory, number theory, discrete probability. 2. Being able to analyze probabilistic algorithms. 3. Develop the ability to model security problems and to write security proofs. 4. Understand fundamental cryptographic primitives including Key Exchange, Digital Signatures, Oblivious Transfer, Public-Key Encryption, Commitment. 5. Understand basic computational problems that are important for cryptography such as the factoring problem, the RSA problem, the discrete-logarithm problem.

Syllabus Information:

-

Recommended Reading List:

1. Steven Galbraith, Mathematics of Public Key Cryptography, https://www.math.auckland.ac.nz/sgal018/crypto-book/crypto-book.html 2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography , http://cacr.uwaterloo.ca/hac/ 3. Victor Shoup, A Computational Introduction to Number Theory and Algebra , http://www.shoup.net/ntb/

Any additional case for support information:

I have been teaching this class for 12 years in University of Connecticut, USA and National and Kapodistrian University of Athens, Greece.