ACE Network Subject Information Guide

Advanced Topics in Cryptography

Semester 1, 2020

Administration and contact details

Host Department	Discipline of Mathematical Sciences, School of Science
Host Institution	RMIT University
Name of lecturer	A/Prof Serdar Boztas
Phone number	03 9925 2285
Email Address	serdar.boztas@rmit.edu.au
Homepage	https://www.rmit.edu.au/contact/staff-contacts/academic-staff/b/boztas-associate-professor-serdar
Name of Honours coordinator	A/Prof Stephen Davis
Phone number	03 9925 2278
Email Address	stephen.davis@rmit.edu.au

Subject details

Handbook entry URL	NA
Subject homepage URL	**NA**
Honours student hand-out URL	NA
Start date:	5 March 2020
End date:	30 May 2020
Contact hours per week:	2
Lecture day and time:	Thursday 6:30pm-8:30pm
Description of electronic access arrangements for students (for example, WebCT)	NA

Subject content

1. **Subject content description**

This course will introduce students of pure and applied mathematics to the field of modern cryptography and the design and analysis of modern cryptosystems as used in current communications and e-commerce security applications. The topics covered symmetric key systems, mainly block ciphers and their design and cryptanalysis, public key cryptosystems including RSA and Elliptic Curve based cryptosystems, and primality testing and factoring.

2. Week-by-week topic overview

- Week 1: Overview of block ciphers: DES, AES
- Week 2: Introduction to the cryptanalysis of block ciphers
- Week 3: Meet-in-the-middle attacks and generic attacks on block ciphers
- Weeks 4-5: Linear cryptanalysis of an SPN cipher
- Weeks 5-6: Differential cryptanalysis of an SPN cipher. Diffusion Methods in block ciphers.
- Week 6: Boolean functions in cryptography.
- Weeks 6-7: A cryptanalytic time memory tradeoff
- Week 7: Review of RSA.
- Week 8: Attacks on RSA. Semantic security. Non-malleable cryptography (time permitting)
- Week 9-10: Arithmetic in Elliptic Curve groups
- Week 10-11: Elliptic curve cryptography. Introduction to primality testing.
- Week 12: Primality testing and factoring

3. Assumed prerequisite knowledge and capabilities

Undergraduate algebra [groups, integer arithmetic, finite fields] , discrete mathematics and probability.

4. Learning outcomes and objectives

Students will acquire a working knowledge of the mathematical techniques used to design and analyse the components of modern cryptosystems. They will be able to translate the mathematical and functional properties of Boolean and vector Boolean functions into a specification of a block cipher substitution or permutation box, and vice versa. Students will be able to understand some cryptanalytic attacks on the RSA cryptosystem.

Students will be able to use the group structure of the additive group over an Elliptic Curve and the discrete logarithm problem to instantiate a public key cryptosystem based on the one-way properties of the discrete logarithm. Students will be able to understand and prove correctness of state of the art algorithms for primality testing and factoring and numerically estimate the security

provided by keys of a certain bitlength in public key algorithms based on the understanding of the above algorithms.

AQF specific Program Learning Outcomes and Learning Outcome Descriptors (if available):

AQF Program Learning Outcomes addressed in this subject	Associated AQF Learning Outcome Descriptors for this subject
Problem Solving - You will have the ability to apply knowledge and skill to characterise, analyse and solve a wide range of problems that arise in the design and analysis of modern cryptosystems.	**S1: cognitive skills to review, analyse, consolidate and synthesise knowledge to identify and provide solutions to complex problem with intellectual independence** **S2: cognitive and technical skills to demonstrate a broad understanding of a body of knowledge and theoretical concepts with advanced understanding in some areas** **A2: to adapt knowledge and skills in diverse contexts**

Learning Outcome Descriptors at AQF Level 8

Knowledge

K1: coherent and advanced knowledge of the underlying principles and concepts in one or more disciplines

K2: knowledge of research principles and methods

Skills

S1: cognitive skills to review, analyse, consolidate and synthesise knowledge to identify and provide solutions to complex problem with intellectual independence

S2: cognitive and technical skills to demonstrate a broad understanding of a body of knowledge and theoretical concepts with advanced understanding in some areas

S3: cognitive skills to exercise critical thinking and judgement in developing new understanding

S4: technical skills to design and use in a research project

S5: communication skills to present clear and coherent exposition of knowledge and ideas to a variety of audiences

Application of Knowledge and Skills

A1: with initiative and judgement in professional practice and/or scholarship

A2: to adapt knowledge and skills in diverse contexts

A3: with responsibility and accountability for own learning and practice and in collaboration with others within broad parameters

A4: to plan and execute project work and/or a piece of research and scholarship with some independence

5. Learning resources

Reference Texts:

Handbook of Applied Cryptography, available online at http://cacr.uwaterloo.ca/hac/

Cryptography: Theory and Practice, Douglas Stinson, 3rd Edition, CRC Press, 2002.

Required Texts:

Lecture notes and other handouts will be provided

6. Assessment

Exam/assignment/classwork breakdown					
Exam	50%	**Lab Assignment**	5%	**3 Class Tests**	**45% total**
Assignment due dates		**Test 1: Week 3**	**Test 2: Week 9**	**Test 3: Week 11**	**Assignment due: Week 11**
Approximate exam date				**Between 10-28 June**	

Institution Honours program details

Weight of subject in total honours assessment at host department	1/8
Thesis/subject split at host department	25% thesis 75% coursework
Honours grade ranges at host department:	
H1	80-100%
H2a	75-79%
H2b	70-74 %
H3	65-69 %