EE609: Modern Cryptography

Module Details

Short Title:	Modern Cryptography DRAFT
Full Title:	Modern Cryptography

Module Code:	EE609	**NFQ Level:**	10	**ECTS Credits:**	5

Valid From:	Academic Session - 2015/16 (September 2015)
Administrator:	Xiaojun Wang
Module Coordinator:	Michael Scott
Description:	This module introduces the student to some exciting new ideas in Modern Cryptography. After a brisk coverage of the required basic number theory, the module will move on to consider elliptic curve crypto and its new offspring, pairing-based crypto. During the course we will develop a crypto software library which will form the basis of lab and project work.

Learning Outcomes:

On successful completion of this module the learner will be able to

1. Implement and appraise modern cryptography algorithms
2. appreciate recent developments in modern cryptographic research
3. Map research developments to real-world problems of security
4. Master the mathematics of elliptic curve cryptography

Pre-requisite learning

Module Recommendations

This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.

No recommendations listed

Requirements

This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.

Students should have basic programming skills, and should be numerate to an undergraduate level. students should have a lap-top computer.

EE609: Modern Cryptography

Module Content & Assessment

Indicative Content

- **Simple Module arithmetic, Quadratic Residues and the Jacobi symbol**
- **Handling big numbers in a computer, Modular inversion and exponentiation**
- **Random Numbers, Prime Numbers, Chinese Remainder theorem**
- **Hard problems from Number theory**
  the discrete logarithm problem and integer factorisation
- **Key Exchange algorithms and Diffe-Hellman**
- **Introduction to Public Key Cryptography**
  Identity based encryption (IBE)
- **Pollards Algorithms for discrete logarithms**
- **Elliptic curves**
  Poit addition and doubling, Weierstrass and Edwards representation
- **The point counting problem. Affine and projective coordinates**
- **Basic elliptic curve algorithms. Some protocols based on elliptic curves. Bitcoin**
- **Supersingular curves and group structure. Extension fields**
- **Cryptographic pairing and their amazing properties. Solving IBE**
- **Finding pairing friendly curves**
  Cocks-Pinch curves and MNT curves, BN curves. Type 1 and type 3 pairings and their properties
- **Novel pairing-based protocols**
  Short Digital Signatures, non-interactive key exchange. Authentication and attribute based cryptography

Assessment Breakdown	**%**
Course Work	100%
End of Semester Formal Examination	0%

Coursework Breakdown

Type	*Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Assignment	Individual projects will be assigned	1,2	40	n/a
In Class Test	End of course test	1,2,3,4	60	n/a

DCU reserves the right to alter the nature and timings of assessment

EE609: Modern Cryptography

Module Workload & Resources

Workload	Full-time hours per semester	
Type	*Description*	*Hours*
Lecture	5 days * 4 hours/day	20
Lab	5 days * 3 hour/day	15
Assignment	Individual projects	60
Independent learning time	Independent learning	30
	Total Workload	125.00

Resources

Essential Book Resources

- **Nigel Smart, *Cryptography, An Introduction***
- **Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography***
- **Henri Cohen and Gerhard Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press**
- **Darrel Hankerson, Alfred Menezes, Scott Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag**

Module Managers & Teachers

Module Coordinators

Semester	*Staff Member*	*Staff Number*
Semester 1	Xiaojun Wang	75020688
Semester 2	Xiaojun Wang	75020688
Autumn	Xiaojun Wang	75020688

Module Teachers

Staff Member	*Staff Number*
No Teacher Staff Assigned	