MODULE TITLE	**Cryptography**	**CREDIT VALUE**	**15**
MODULE CODE	**MTH3026**	**MODULE CONVENER**	**Dr Gihan Marasingha (Coordinator)**

DURATION: TERM	**1**	**2**	**3**
DURATION: WEEKS	**0**	**11 weeks**	**0**

Number of Students Taking Module (anticipated)	**116**

DESCRIPTION - summary of the module content

Cryptography is the mathematical art and science of maintaining information security. In this module, you will learn practical algorithms for encrypting plain messages into secret messages. These algorithms ranges from the simple ciphers used in ancient Rome to the sophisticated modern ciphers that secure worldwide banking transactions and diplomatic communications.
You will study two broad classes of cryptosystems: symmetric and asymmetric. Modern symmetric ciphers such as AES (the Advanced Encryption Standard) have their mathematical basis in linear algebra and field theory, whereas asymmetric ciphers such as RSA and ElGamal are founded on number theory and group theory.
Knowing how to crack asymmetric cryptosystems requires developing methods for factorising large numbers and testing numbers for primality. These methods are at the heart of modern attempts to break secret codes.
The module concludes with an introduction to elliptic curve cryptography, a topic with connections to Algebraic Curves (MTHM029).
You will be given a brief introduction to the computer programming language Python in the particular context of solving cryptographic problems.
Prerequisite module: MTH3004.

AIMS - intentions of the module

The aim of this module is to apply number theory, linear algebra, and field theory to problems in the real world where it is important to transmit information securely. For example, cryptography is used in banking, and is traditionally applied in military science.

INTENDED LEARNING OUTCOMES (ILOs) (see assessment section below for how ILOs will be assessed)

On successful completion of this module, ***you should be able to***:

Module Specific Skills and Knowledge:

1 formulate encryption as a mathematical problem;

2 define and be able to determine the complexity of algorithms using the Landau notation;

3 describe and apply the principles of block ciphers with particular examples including the Vigenère, affine, and Hill cipher;

4 describe and apply the field theoretic underpinnings of the AES cryptosystem;

5 demonstrate an understanding of the principles of asymmetric key cryptography;

6 describe, apply and prove theorems concerning with asymmetric key algorithms such as Diffie-Hellman key exchange, the ElGamal PKC and the RSA PKC;

7 describe the discrete logarithm problem;

8 describe, apply and prove theorems concerning methods for the solution of discrete logarithm problems including: the baby-step, giant-step algorithm, the Pohlig-Hellman algorithm;

9 describe, apply and prove theorems concerning factorisation methods, including Fermat factorisation, Pollard’s p-1 method, Pollard’s rho method, and Lenstra’s elliptic curve method;

10 describe, apply and prove theorems concerning primality testing methods, including the Fermat and Miller-Rabin primality tests;

11 understand the principles of digital signatures;

12 describe, apply, and prove theorems concerning digital signature algorithms including the ElGamal and RSA digital signature schemes;

13 describe the arithmetic of elliptic curves and demonstrate an understanding of elliptic curve cryptography;

14 describe classes of cryptographic attack (including known plaintext attack, adaptive chosen ciphertext attack, etc.) and determine whether a given cryptosystem is vulnerable to a particular class of attack;

15 perform sophisticated cryptographic computations, either by hand or using Python and the Jupyter notebook interface.

Discipline Specific Skills and Knowledge:

16 appreciate how to apply number theory, linear algebra, field theory, and group theory to real-world problems;

17 prove theorems concerning the effectiveness and complexity of algorithms.

Personal and Key Transferable/ Employment Skills and Knowledge:

18 show an appreciation of how concrete problems typically require abstract theories for their solution;

19 display an ability to analyse algorithms.

SYLLABUS PLAN - summary of the structure and academic content of the module

- introduction to cryptography, history of cryptography; symmetric and asymmetric cryptosystems; some simple examples;
- block ciphers (Vigenère, affine, Hill); block cipher modes of operation (ECB, CBC);
- constructing finite fields and the AES (Advanced Encryption Standard);
- complexity of algorithms;
- Diffie-Hellman key exchange; the ElGamal PKC (public key cryptosystem);
- cryptanalysis of discrete logarithm-based problems – Shank’s baby-step, giant-step and the Pohlig-Hellman algorithm;
- the RSA cryptosystem;

- trial division and Fermat factorisation;
- other factorisation methods: Pollard’s p-1 method, Pollard’s rho method;
- primality testing: Fermat and Miller-Rabin primality tests;
- authentication: ElGamal and RSA digital signature schemes;
- the unit circle group;
- the elliptic curve group; elliptic curve Diffie-Hellman; Lenstra’s elliptic curve method for integer factorisation.

LEARNING AND TEACHING

LEARNING ACTIVITIES AND TEACHING METHODS (given in hours of study time)

Scheduled Learning & Teaching Activities	33.00	Guided Independent Study	117.00	Placement / Study Abroad	0.00

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled learning and teaching activities	33	Lectures/example classes
Guided independent study	117	Lecture and assessment preparation; private study

ASSESSMENT

FORMATIVE ASSESSMENT - for feedback and development purposes; does not count towards module grade

Form of Assessment	Size of Assessment (e.g. duration/length)	ILOs Assessed	Feedback Method
Example sheets	4 x 10 hours	All	Solutions made available through ELE

SUMMATIVE ASSESSMENT (% of credit)

Coursework	20	Written Exams	80	Practical Exams	0

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of Credit	Size of Assessment (e.g. duration/length)	ILOs Assessed	Feedback Method
Coursework 1- based on questions submitted for assessment	10	15 hours	All	Annotated script and written/verbal feedback
Coursework 2- based on questions submitted for assessment	10	15 hours	All	Annotated script and written/verbal feedback
Written Exam – closed book	80	2 hours (Summer)	All	Written/verbal on request, SRS

DETAILS OF RE-ASSESSMENT (where required by referral or deferral)

Original Form of Assessment	Form of Re-assessment	ILOs Re-assessed	Time Scale for Re-assessment
Written Exam *	Written Exam (2 hours)	All	August Ref/Def period
Coursework 1 *	Coursework 1	All	August Ref/Def period
Coursework 2 *	Coursework 2	All	August Ref/Def period

*Please refer to reassessment notes for details on deferral vs. Referral reassessment

RE-ASSESSMENT NOTES

Deferrals: Reassessment will be by coursework and/or written exam in the deferred element only. For deferred candidates, the module mark will be uncapped.
Referrals: Reassessment will be by a single written exam worth 100% of the module only. As it is a referral, the mark will be capped at 40%.

RESOURCES

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of information that you are expected to consult. Further guidance will be provided by the Module Convener

ELE – http://vle.exeter.ac.uk

Reading list for this module:

Type	Author	Title	Edition	Publisher	Year	ISBN	Search
Set	Hoffstein, J., Pipher, J. & Silverman, J.H.	An introduction to mathematical cryptography	2nd	Springer	2014	978-1493917105	[Library]
Set	Koblitz, Neal	A course in Number theory and Cryptography	Graduate Text in Mathematics	Springer	1994		[Library]
Set	Buchmann, J	Introduction to Cryptography	2nd	Springer	2004	978-0387207568	[Library]

CREDIT VALUE	15	ECTS VALUE	7.5
PRE-REQUISITE MODULES	MTH3004		
CO-REQUISITE MODULES			
NQF LEVEL (FHEQ)	6	AVAILABLE AS DISTANCE LEARNING	No
ORIGIN DATE	Tuesday 10 July 2018	LAST REVISION DATE	Thursday 26 January 2023
KEY WORDS SEARCH	Fermat's little theorem; Miller-Rabin test; cryptosystems (symmetric cryptosystems and public key cryptosystems); encryption; decryption; RSA - and related cryptosystems; discrete logarithmic problems.		