LTCC Proposed Course

Title: Cryptography and Mathematical Ciphers

Basic Details:

- Core Audience: 1st yr (pure and applied)
- Course Format: **extended** (5 x 2hr lectures)

Course Description:

- Keywords: public-key ciphers, RSA, ElGamal cipher, elliptic curve cryptography, NTRU encryption, post-quantum cryptography

- Syllabus: This course will introduce mathematical, number theoretic concepts needed for modern mathematical ciphers that are used in today's everyday online communication, in particular public-key ciphers such as RSA, ElGamal and Elliptic Curve Cryptography (ECC). We will also discuss the underlying principles that make these ciphers secure and how they could potentially be broken in the future, leading us to the development of lattice-based ciphers (e.g. NTRU) and post-quantum cryptography.

- Recommended reading: 'An introduction to mathematical cryptography' by J. Hoffstein, J. Pipher and J. H. Silverman (Springer, 2008)

- Prerequisites: (elementary) number theory, basic algebra (groups, rings, fields)

Format:

- No of discussion/problem sheets: 4
- Electronic lecture notes: will be provided in or after the lecture

Lecturer Details:

- Lecturer: Dr Thomas Kecker
- Lecturer home institution: University of Portsmouth, School of Mathematics and Physics
- Lecturer e-mail: thomas.kecker@port.ac.uk