School of Mathematics

Course 374 — Cryptography & Information Theory 1998-99
(JS & SS Mathematics)

Lecturer: Michael Purser & Timothy Murphy

Requirements/prerequisites:

Duration: 21 weeks

Number of lectures per week: 3

Assessment: Cryptography will account for 60% of the overall mark; Information Theory for 40%. Cryptography will be marked entirely by Exam. There may be a Project element in Information Theory.

End-of-year Examination: One 3-hour examination

Description:
This course is in 2 independent parts: Cryptography, given by Dr Purser; and Information Theory, given by Dr Murphy.

Dr Pursers's part of the course will be marked by Examination; Dr Murphy's part will also be marked by Examination, with a possible contribution by Project.

Dr Purser's part of the course will start in November.

1 Cryptography

This course discusses cryptography with particular reference to computer networks.

Topics (not necessarily in order of appearance):

- Introduction—Confidentiality and Authenticity
- Shannon's Theory
- Block Encryptors and Stream Encryptors
- ECB, CBC, CFB modes
- Integrity checks
- MDC's and MAC's
- Identification, Authentication and Authorisation
- Access control procedures: 1-way, 2-way
- Public (Asymmetric) Key Crytpology *vs* Private (Symmetric) Key Cryptology
- Non-repudiation
- 3-way access control

- Digital signatures
- Diffie-Hellman Key Exchange
- Some algorithms
  - Vigénère, Vernam
  - Enigma
  - DES
  - A stream encryptor based on maximum length sequences
  - RSA
  - IDEA
  - FIAT/SHAMIR
  - Hashing algorithms
- Relevant Mathematics
  - Generating Primes
  - Testing Primes
  - Factorising
  - Random Numbers
  - Discrete Logarithms
- Cryptanalysis
  - Statistical Analyses
  - Brute force
  - Differential Cryptanalysis
- Key Management
  - Key Distribution
  - Certification
  - Sharing Keys
  - PINs
  - Chipcards

2 Information Theory

This course will cover *Algorithmic Information Theory*, a subject which marries Shannon's original Statistical Information Theory to the concepts of computability and Turing machines.

According to Algorithmic Information Theory, the *informational content*, or *entropy*, of a string may be measured by the minimum length to which the string can be compressed.

Notes for the course are available on the Maths Unix System in very"/usr/local/pub/AlgorithmicInformationTheory". Read `README` before printing them out.

June 10, 1998