School of Mathematics

Course 374 — Cryptology 2004-05
(JS & SS Mathematics)

Lecturer: Dr. T. G. Murphy & Dr. M. Purser

Requirements/prerequisites:

Duration: 21 weeks

Number of lectures per week: 3

Assessment:

End-of-year Examination: 3-hour end of year exam

Description:

Topics to be covered by Dr. Murphy. Still to be added.

Topics to be covered by Dr. Purser. This part of course 374 will probably begin in the third week of the Michaelmas term. Details will be announced later.

- **Introduction**

  The security of computer-based information, stored or transmitted.

  Threats: Modification, Masquerade, Leakage, Replay, Repudiation, Traffic analysis, etc.

  Services:

  - Confidentiality (message, traffic),
  - Authenticity (Integrity, Proof and Non-repudiation of Origin or Reception or Delivery, etc.)

  Identification, Secure access management (handshakes), Biometrics, etc.

  Secret keys versus secret algorithms.

  Generation, storage and transmission of secret keys.

  Examples:

  - Symmetric encryption: Caesar's cypher.
  - Integrity: CRC/Hash.
  - Authentication: Keyed hash, DES MAC.

  Other aspects: Steganography, Chaffing Winnowing, Threshold crypto, etc.

  Standard attacks: Known plaintext/cyphertext; Chosen plaintext/cyphertext; Brute force.

  Long messages, All-or-nothing transform.

- **Concepts**

  Shannon's theories: Unicity key lengths and distances, Perfect secrecy.

  Symmetric key cryptography: Encryption and MACs (message authentication checks).

  Asymmetric Key cryptography: Encryption and digital signatures.

  Distribution and certification of public keys.

  Time-stamping.

  Trusted third parties (TTPs).

- **Symmetric/Secret Key Cryptology**

  History: Substitution, permutation, involution.
  Vigenere, Beaufort, Polyalphabetic, Jefferson Wheel, Wheatstone Disc, Enigma

  DES (Data encryption standard), Triple-DES, IDEA etc.

  The AES Project

  Mars, Twofish, RC6, Serpent, Rijndael

  Encryption modes: ECB, CBC, CFB, etc.

  Integrity checks: MACs

  Stream cyphers.

  Statistical crypt-analysis, shift-and-correlate, etc.

- **Random numbers and sequences**

  For symmetric keys; as ideal cyphertext.

  Random number generators: LCGs, LFBSRs and MLSs, BBS, de Bruin sequences, etc.

  Tests for randomness: String lengths, Chi-square.

- **Asymmetric Public Key Cryptography**

  Concept and invention of public-key crypto (Ellis, Cocks)
  (Certification of public keys)

  Bi-prime crypto

  Modular arithmetic: Fermat, Euler, primitivity, totient function

  The discrete logarithm (DL) problem

  Diffie-Hellman and RSA

  Rabin encryption

  Very large integers and their implications.

- **Asymmetric system techniques**

  RSA parameters and frustrating attacks.

  Primality testing: Rabin, Carmichael numbers

RSA security: order of the group.

Modular inverses, Euclid, continued fractions.

Chinese remainder theorem (CRT)

Speeding up the arithmetic: Karatsuba, Montgomery, small exponents, etc.

Other algorithms:

- DSA/SHA-1 signature standard.
- RPK, MTI/A0, MTI/C0, MQV, Quadratic residues, Fiat-Shamir, Elgamal

Other techniques: Knapsack, Lucas series, elliptic curves, finite quaternions, affine maps, etc.

Holding private keys securely.

- **Hash functions**

  Desiderata

  SHA-1, square-mod, MDC, RIPE-MD, RIPE-160, etc.

  Keyed hash functions

- **More crypt-analysis**

  Differential crypt-analysis (Bihar-Shamir)

  Linear crypt-analysis (Matsui)

  Factorising: Fermat, the birthday paradox and Pollard Monte Carlo, Pollard (p+1).

  Sub-exponential complexity and the use of factor bases.

  Dixon's method, Quadratic sieve, Continued fractions, Number field sieve.

  The DL problem, Coppersmith et al.

The course will atempt to cover most of the above topics, some obviously less thoroughly than others.

September 8, 2004