School of Mathematics

Course 374 — Cryptography   2008-09
(JS & SS Mathematics)

Lecturer: Dr. M. Purser

Requirements/prerequisites:

Duration: 19 weeks

Number of lectures per week: 3

Assessment:

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

Description:

1. **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: What you know, what you have, what you are. Secure access management (handshakes), Biometrics.

   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, Threshold crypto.

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

   Long messages, All-or-nothing transform.

2. **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).

   Anonymity

3. **Symmetric or 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 The winner Rijndael

    Encryption modes: ECB, CBC, CFB, etc.

    Integrity checks: MACs

    Stream cyphers.

    Statistical crypt-analysis, shift-and-correlate.

4. **Random numbers and sequences**

    For symmetric keys; as ideal cyphertext.

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

    Tests for randomness: String lengths, Chi-square.

5. **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.

6. **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.

    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

    Holding private keys securely.

7. **Hash functions**

   Desiderata SHA-1, square-mod, MDC, RIPE-MD, RIPE-160 The competition for replacing SHA Keyed hash functions

8. **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, Introduction to the Number Field Sieve.

   The DL problem, Coppersmith et al.

The course will attempt to cover most of the above topics, some obviously less thoroughly than others. The best guides to coverage are the exam papers of the last decade.

Lecture notes available at:
`http://www.maths.tcd.ie/~mpurser`

February 28, 2010