School of Mathematics

Course 374 — Cryptography
(JS & SS Mathematics )

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

Requirements/prerequisites:

Duration: 21 weeks

Number of lectures per week: 3

Assessment:

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

Description: The course will be in two parts: Dr Purser will lecture on Cryptography for 2 hours per week, and Dr Murphy will lecture on Elliptic Curves for Cryptography for 1 hour per week.

Outline of Dr Purser’s course on Cryptography

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, Secure access management (handshakes), Biometrics, etc.
- Secret keys versus secret algorithms.
- Generation, storage and transmission of secret keys.
- Examples: Symmetric encryption: Caesars 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.

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/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.

4. 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.

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, etc.
- Holding private keys securely.

7. Hash functions

- Desiderata
- SHA-1, square-mod, MDC, RIPE-MD, RIPE-160, etc.
- 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.
- Dixons method, Quadratic sieve, Continued fractions, 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.

**Outline of Dr Murphy’s sub-course on Elliptic Curves for Cryptography**

This part of the course will study elliptic curves over finite fields, and their use in cryptography.

1. Overview

- The discrete log problem for $F_p$
- The discrete log problem for abelian groups
- Elliptic curve cryptography

2. Preliminaries

- Finite abelian groups
- Finite fields
- P, NP and NP-complete
3. Elliptic curves
   - The Weierstrass standard form
   - Addition
   - Isogenies

4. Elliptic curves over finite fields
   - Examples
   - Hasse’s theorem
   - Shooj’s algorithm

October 9, 2006