KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
COLLEGE OF COMPUTER SCIENCES & ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

COE 509: Applied Cryptosystems: Techniques and Architectures

Term 072 (Second Term 2007)

Instructor Dr. Adnan Gutub. Office: 22/145 Phone: 1723 Email: gutub@kfupm.edu.sa

Catalogue Description:

Introduction to encryption and information hiding.
Mathematical Foundation of Cryptography.
Private and Public key Cryptosystems.
Key Protocol and Management.
Ciphers.
Advanced Encryption Standard.
Digital Signatures.
Elliptic Curve Cryptosystems.
Architectures of Cryptosystems and Processors.

Prerequisite:

Consent of Instructor.

Helpful Books:

1. Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
2. Modern Cryptography Protect Your Data with Fast Block Ciphers, Nik Goots, Boris Izotov, Alex Moldovyan, Nik Moldovyan
3. Cryptography Theory and Practice, Doug Stinson

Grading Policy:

Exams & Quizzes 30%

- Quizzes
- Midterm
- Final

Assignments 20%

Steganography Paper 20%

Week 3: Proposed Idea & References to be submitted
Week 6: Report
Week 7: Presentation

Crypto Project 30%

(topic based on interest)

Week 9: Proposed Idea and References to be submitted
Week 13: Report
Week 15: Presentation

Covered Lectures Topics :

- Introduction (Week 1)
  - Concepts; Definitions; Encryption & Info hiding
- Steganography (Week 1-2)
  - Applications; Main aspects; Difference: Cryptography and Watermarking; Stego model; Greyscale images steganography
  - S-tools; RGB image steganography; Pixel indictor technique; Text steganography; Arabic text steganography; Kashida & Diacritics Stego Methods.
- Overview of Cryptography (Week 3)
  - Terminology; Crypto model & Attack means; Kerckhkoffs principle; Mono-alphabetic ciphers; Modern ciphers property; Symmetric/Asymmetric key cryptography & applications; Public Crypto Spoofing Attack (Man-in-middle); Key management issues
  - Authentication; Aspects of PKC; Key space & Brute force; Unbreakable Cryptosystem; Crypto Applications; Hash Functions; Security Risks & Attacks
- Classic Cryptosystems (Week 4-5)
  - Modulo & Ring characteristics; Modulo arithmetic properties
  - Substitution; Transposition; Enigma Machine; Shift; Affine; Vigenere
  - Block (Hill); Detailed example of cryptography using modulo computations
  - Properties of Good Cryptosystems; Vernam (one time pad)
  - Random number generation; Stream Ciphers; LFSR; Nonlinear Combination Generator (Geffe generator); Synchronous/Asynchronous Stream Ciphers; SEAL
- RSA & Number Theory (Week 6-8)
  - Diffie Hellman Key distribution; trapdoor one-way function; PKC & Standards; Divisibility; Primes; GCD; Euclidean algorithm & its extension; Congruence Classes; Chinese Remainder Theorem; Euler's theorem; Exponentiation; Primitive roots
  - RSA encryption & decryption; RSA digital signature; RSA Key lengths; RSA security & attack
  - Finite Fields; Group properties - abelian - cyclic; Order of groups; Galois Fields; Polynomial Arithmetic in general and in $GF(2^n)$
- Steganography Paper Presentations (Week 9)
- RSA Hardware Architectures (Week 9-10)
  - RSA Implementations Principles; 90's RSA & Modular arithmetic designs; RSA exponentiation (MSB first & LSB first) algorithms & architectures comparisons
  - RSA Multiplication; Montgomery Multiplication Princeples; Montgomery Multiplication Hardware algorithms & architectures; Expandable designs; Scalable designs; Improving multiplication through fast adders.
- Elliptic Curve Cryptography (ECC) (Week 11-12)
  - What & Why ECC?; Benefits, Applications, Equivalent key sizes; Security Strength

    - Some theory of Elliptic Curves (EC); EC & finite fields; EC Point properties & operations; EC Scalar multiplications; EC Discrete Logarithm Problem (ECDLP); EC Generator Point
    - ECC Application: ECDH, EC Encryption/Decryption, ECDSA, ElGamal ECC
    - EC Projective Coordinate Systems
- ECC Hardware Issues (Week 13)
    - GF(p) & GF(2^k) ECC Architecture Designing: Single/Multiple/Pipelined Multiplier Desings
    - Montgomery Modular Inverse Hardware & Scalability; Multi-bit shifting Invsrsion Hardware; Unified Montgomery Inversion in GF(p) & GF(2^k)
- Symmetric Key Cryptosystems (Week 14)
    - DES Encryption/Decryption; AES Encryption/Decryption
- Crypto Remarks (Week 15)
    - Students Research Presentations