M.Tech (CLIS)

Advanced Cryptography (IADC240C)

Objective:

This course provides an overview of modern cryptographic theories and techniques, mainly focusing on their application into real systems. Topics include number theory, probability and information theory, computational complexity, symmetric and asymmetric cryptosystems, one-way functions, block and stream ciphers, public key infrastructure (PKI), cryptographic protocols in many real systems.

Detailed Syllabus:

Unit 1: Overview of Cryptography
Introduction, Information security and cryptography, Basic terminology and concepts, Symmetric-key encryption , Digital signatures, Public-key cryptography, Hash functions, Protocols and mechanisms, Key establishment, management, and certification, Pseudorandom numbers and sequences, Classes of attacks and security models.

Unit 2: Mathematical Background
Probability theory , Information theory, Complexity theory, Number theory, Abstract algebra, Finite fields, The integer factorization problem, The RSA problem, The Diffie-Hellman problem, Composite moduli.

Unit 3: A quick introduction to groups, rings, integral domain and fields (including: Lagrange theorem, Structure of cyclic and abelian groups, isomorphism theorems). 4-Lectures

Unit 4: Fields, Characteristic of a field, prime fields, Arithmetic of polynomials over fields. Field extensions, Galois group of a field extensions, Fixed field and Galois extensions. Minimum polynomial, Construction of fields with the help of an irreducible polynomial. Splitting field of a polynomial, Separable polynomial and Separable extensions. Construction of finite fields and their structure. Enumeration of irreducible polynomials over finite fields. Fundamental theorem of Galois Theory. 8-Lectures

Unit 5: Cyclotomic extensions, Geometric constructions and Galois theory of Equations (Statement only of Abel Ruffini), Solving Cubic and Bi-quadratic polynomials using radicals. 8-Lectures

Unit 6: Key Establishment Protocols
Introduction, Key transport based on symmetric encryption, Key agreement based on symmetric techniques, Key transport based on public-key encryption, Key agreement based on asymmetric techniques, Secret sharing, Key Management Techniques, Techniques for distributing public keys, Techniques for controlling key usage, Key management involving multiple domains.

Books

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography” CRC Press
2. Cryptography and Network Security: Principles and Practice (ISBN 0131873164), 4/e, by William Stallings
3. B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd Edition, John Wiley & Sons, 1995.
4. Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2002.
5. Mihir Bellare and Phillip Rogaway, “Introduction to Modern Cryptography”
6. Field and Galois Theory, By Patrick Morandi GTM
7. Field and Galois Theory, By J.M. Howie (Paperback)
8. Galois Theory, Lecture notes by Emil Artin
9. Galois Theory,   TIFR Lecture notes
10. Galois Theory by H.M. Edward (GTM)
11. Algebra , By M. Artin

Note: Subject to Change