IT325 - Introduction to Cryptography (3 – 0 – 0 – 3)

Instructor: Dr. Manik Lal Das
Office: 2103, Faculty Block 2, Extn. 617
Email: maniklal_das@daiict.ac.in

Course Description
Cryptography is concerned with the mathematical, algorithmic, and implementation aspects of information and network security. It is one of the core technologies for securing applications ranging from “border security” to “consumer electronics”. After completion of this course, students will display a breadth of knowledge in applied cryptography and be able to build secure systems for real-world problems.

Content
- **Classical Cryptography**: Mono-alphabetic; poly-graphic; poly-alphabetic; rotor machine.
- **Secret Key Cryptography**: Feistel structure; block ciphers - DES, AES, IDEA; stream ciphers – LFSR, RC4.
- **Modes of operation**: ECB, CBC, CFB, CTR, OFB.
- **Data Integrity**: Hash functions – MD5, SHA; Message Authentication Codes (MAC).
- **Public Key Cryptography**: Integer Factorization Problems (IFP); Discrete Logarithm Problems (DLP); Elliptic Curve (EC) Discrete Logarithm Problems; Bilinear Pairings; RSA; Diffie-Hellman; ElGamal; DSA; ECDSA; Identity-based cryptography.
- **Key Management**: Public Key Infrastructures

Book
- **Introduction to Cryptography with Coding Theory** -- Washington & Trappe [Pearson].

Grading policy
First and Second in-semester exams: (20+20) %
End-semester exam: 40 %
Quizzes/Class participation: 20 %

Attendance Policy
Students’ attendance would be taken randomly. A measure of ≥ 60% attendance (from classes, quizzes, in-semester exams) would be followed to consider students status as Regular. Less than 60% attendance means Irregular student (except student has health problem) and such students may face poor performance at the end of the course.