|  |  |
| --- | --- |
|  |  |
|  |

|  |  |
| --- | --- |
| MONO | **DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**  **NATIONAL INSTITUTE OF TECHNOLOGY PATNA**  Ashok Raj Path, PATNA 800 005 (Bihar), India |
| Phone No.: 0612 – 2372715, 2370419, 2370843, 2371929, 2371930, 2371715 Fax – 0612- 2670631 Website: [www.nitp.ac.in](http://www.nitp.ac.in/) |

***CSX436 Cryptography***

**L-T-P-Cr: 3-0-0-3**

**Pre-requisites:** Prior knowledge of fundamentals of Graph theory, Number theory.

**Course Objectives:**

1. To impart knowledge of cryptography in the recent days.
2. To make students understand the concepts and technologies behind cryptography.
3. To impart ability to design and implement of cryptographic algorithms for data security.
4. To make students aware of cryptanalysis or breaking of ciphers.

**Course Outcomes:**

At the end of the course, a student should:

|  |  |  |
| --- | --- | --- |
| Sl. No | Outcome | Mapping to PO |
|  | Understand the state-of-the-art cryptographic algorithm | PO2, PO3 |
|  | Explain technologies behind cryptography | PO2, PO3 |
|  | Develop the ability to design cryptographic algorithms | PO2, PO3,PO4 |
|  | Analyze the security of cryptographic algorithms performance | PO2, PO3 |
|  | Learn to effectively combine techniques and ideas from different areas of computer science | PO2,PO3, PO4 PO6, PO12 |

**UNIT I: Lectures:14**

Foundation- Integer and modular arithmetic, matrices, traditional symmetric-key ciphers- substitution, transposition, stream and block ciphers, algebraic structures- group, ring, field theory, GF(2n) fields, modern block and stream ciphers. Introduction to modern symmetric key ciphers-modern block and stream ciphers, linear Algebra. Mathematical Background: Shannon’s Theory, Computational Complexity, Finite Fields, Number Theory. Luby Rackoff’s Construction and the Feistel Cipher. Concept of Pseudo-Random Functions.

**UNIT II: Lectures:6**

Symmetric-Key encipherment - Data Encryption Standard (DES). Structure, analysis, multiple DES and security. Advanced Encryption Standard(AES)- introduction, transformation, key expansion, ciphers, analysis. Use of modern block and stream ciphers. Attack Models for Ciphers: Linear, Differential, Impossible Differential, Slide Attacks. Design of Substitution Boxes (S-Boxes), Other block ciphers, stream ciphers: RC4, A5/1

**UNIT III: Lectures:8**

Asymmetric-Key Encipherment- One way and Trapdoor Functions, Primes, primality testing, factorization, Chinese remainder theorem, quadratic congruence, exponentiation and logarithm. RSA cryptosystem, Rabin Cryptosystem, Elgamal Cryptosystem, Elliptic Curve Cryptosystems.

**UNIT IV: Lectures:11**

Message Integrity and Message Authentication- Message Integrity, Random Oracle Model, Message Authentication Code (MAC), Cryptographic Hash Functions- SHA-512, WHIRLPOOL, Digital Signature- process, services, attacks, and schemes – RSA, Elgamal, Schnorr, DSS, Elliptic Curve Digital Signature Scheme. Applications. Entity Authentication: Introduction, passwords, challenge-response, zero knowledge – Fiat Shamir, Feige-Fiat-Shamir, Guillou - Quisquater Protocol, biometrics.

**UNIT V: Lectures:3**

Recent topics- Homomorphism: Definition, Basics, Types of homomorphic encryption: Partial and Full Homomorphism. Paillier Cryptosystem.

**Text/Reference Books:**

1. Cryptography & Network Security by Behrouz A. Forouzan,2nd Edition, McGraw Hill
2. Cryptography and Network Security, by William Stallings.
3. Cryptography Theory and Practice, Third Edition, by Douglas Stinson.
4. Everyday Cryptography By Martin, Oxford University Press