राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- Date:

CS74135: Applied Cryptography

L-T-P-Cr: 3-0-2-4

Pre-requisites: Prior knowledge of fundamentals of Computer Networks, Cryptography

Objectives/Overview:

- To impart knowledge of recent developments in applied cryptography.
- To make students understand the concepts and technologies behind Cryptographic protocols.
- To impart ability to design and implement security protocols for an organization.
- To make students aware of privacy and security issues that arise in practice from areas like cloud computing, databases, surveillance and finance.

Course Outcomes:
At the end of the course, a student should:

Sl. No	Outcome
1.	Understand how state-of-the-art cryptographic protocols work
2.	Explain technologies behind cryptography
3.	Develop the ability to design cryptographic protocols
4.	Analyze the security of cryptographic protocols
5.	Learn to effectively combine techniques and ideas from different areas of computer science

UNIT I: **Lectures: 6**

Mathematical Foundation- Integer and modular arithmetic, matrices, algebraic structures- group, ring, field theory, Shannon's Theory, Computational Complexity, Finite Fields, Number, Theory. Luby Rackoff's Construction and the Feistel Cipher. Concept of Pseudo-Random Functions, linear Algebra.

UNIT II: **Lectures: 8**

Symmetric key cryptography, Block ciphering techniques, DES, AES, 3DES, Blowfish, Stream ciphers, RC4, SEAL, A5/1, hash algorithms, MD5, N hash, SHA1, Public key algorithms, Knapsack, RSA, ECC.

UNIT III: **Lectures: 6**

Cryptographic protocols, Key Exchange, Authentication, Formal analysis of authentication and key exchange protocols, Multiple-Key Public-Key Cryptography, Secret Splitting, Secret Sharing, Cryptographic Protection of Databases, Timestamping Services, Subliminal Channel, Digital

Signature, Proxy Signatures, Group Signatures, Fail-Stop Digital Signatures, Computing with Encrypted Data, Key Escrow.

UNIT IV: **Lectures: 8**

Advanced Protocols- Zero-Knowledge Proofs, Blind Signatures, Identity based Public key cryptography, Oblivious Transfer, Oblivious signatures, Simultaneous Contract Signing, Digital Certified Mail, Simultaneous Exchange of secrets, Secure Multiparty Computation, Anonymous Message Broadcast, Digital Cash.

UNIT V: **Lectures: 7**

Key-Exchange Algorithms- Diffie Hellman, Station-to-Station Protocol, Shamir's Three-Pass Protocol, COMSET, Encrypted key Exchange, Fortified Key Negotiation, Key Escrow

UNIT VI: **Lectures: 7**

Secure application Design, Writing secure software, J2EE security, Windows .NET Security, Controlling application Behavior

Text/ Reference Books:

1. Applied cryptography: protocols, algorithms, and source code in C, Bruce Schneier, John Wiley & Sons, 2007
2. Everyday Cryptography By Martin, Oxford University Press
3. Information Security: The Complete reference By Mark Rhodes Ousley, 2nd Edition. McGraw Hill
4. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management; Hossein Bidgoli, John Wiley & Sons
5. The Basics of Information Security, 2nd Edition; J Andress, Syngress Press; 2014