Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: CSXXX

2. Course Title: Cryptographic Protocols

3. Per Week Lectures: 3(L), Tutorial: 0 (T), Laboratory: 0 (P), Additional Hours [0-2]: 0 (A), **Credits (3-0-0-0-9)**: **Duration of Course: Full semester**

4. Proposing Department: Computer Science and Engineering

Other Departments/IDPs which may be interested in the proposed course: Mathematics, Electrical Engineering

Other faculty members interested in teaching the proposed course: Nitin Saxena

5. Proposing Instructor(s): Angshuman Karmakar (angshuman@iitk.ac.in)

7. Course Description:

A) Objectives: This course explores the design, analysis, and application of cryptographic protocols, which are essential for securing communication, authentication, and privacy in computer networks. Students will study fundamental cryptographic concepts such as encryption, digital signatures, hash functions, and zero-knowledge proofs, along with advanced protocols like secure multi-party computation. This course focuses on the constraints, security arguments, hard mathematical problems, and instantiations of cryptographic primitives. A student upon taking this course will be able to analyse the security of different cryptographic primitives and will also be confident to design new cryptographic primitives.

B) Contents (preferably in the form of 5 to 10 broad titles):

Lecture-wise break-up (considering the duration of each lecture is 50 minutes)

Serial	Broad title	Topics	No of lectures
1	Foundations of cryptographic protocols [1, 2, 3]	• Cryptology basics • Probability and Number theory • Randomness and pseudorandom generators • Security models: Adversarial models & proof techniques • Common attacks on cryptographic protocols	7
2	Key exchange protocols [3,4,5]	• Diffie-Hellman key exchange & variants • Authenticated key exchange	3
3	Commitment schemes [2, 5, 6]	• Definition and security properties • Pederson commitment	3

		• Using cryptographic hash functions • Using discrete log setting • Homomorphic commitments	
4	Identification protocols[2, 5, 6]	• Password based schemes • One-way hash chains • Basic challenge response using symmetric/asymmetric schemes • Zero knowledge identification protocols • Witness hiding identification protocols	3
5	Zero-Knowledge proofs and authentication [2, 6]	• Sigma Protocol • Compositions of Sigma protocols • Non-interactive Zero-Knowledge	4
6	Threshold cryptography and Secure multi-party Computation [2, 6]	• Additive and Shamir secret sharing • Basics of MPC, Brever triplet • Verifiable secret sharing • Publicly verifiable secret sharing • FROST: threshold signature based on Schnorr-style	4
7	Digital signature schemes [3, 4, 5, 6]	• Basic constructions from Full Domain Hash paradigm, and Identification scheme • Unforgeability property, key only attack (KOA) • Designing quantum-safe signatures using Multi Party Computation-in-the-Head (MPCitH) framework	6
8	Blind Signatures [4, 5]	• Security properties • Three-pass protocol, Schnorr framework for designing BS, • Two-pass protocol, Fischlin's framework • ROS problem, and its applications to BS	6
9	Advanced Topics in Cryptographic Protocols [2, 6]	• Secure voting protocols • Private information retrieval • Anonymous communication networks (Tor, Mixnets)	4

C) Recommended pre-requisites, if any: Mandatory: Discrete mathematics, algorithms, theory of computations, programming knowledge

Desirable: Basic knowledge of cryptography

D) Short summary for including in the Courses of Study Booklet: Design of cryptographic primitives, principles of cryptography design, security in computer systems, cryptographic protocols.

7. Recommended text/reference books:

1) *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, Cambridge University Press, 2008.
2) *Handbook of Applied Cryptography* by Alfred Menezes, Paul C. van Oorschot, and Scott Vanstone, 1997.
3) *Cryptography: Theory and Practice* by Douglas Stinson and Maura Paterson, 4th edition, CRC Press, 2018.
4) *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC Press, 2007.
5) *Cryptography: An Introduction* by Nigel Smart, McGraw-Hill, 2003.
6) *Modern Cryptography: Theory and Practice* by Wenbo Mao, first edition, Pearson Education, 2004.

8. Any other remarks: None

Dated: 28/02/2025 Proposer: Angshuman Karmakar

Dated: DPGC Convener:

The course is approved / not approved

Chairman, SUGC

Dated: