Indian Institute of Technology Kanpur

Proposal for a New Course

1. Course No: xxxxx
2. Course Title: Cryptography and Digital security: Theory and Practice
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, Somitra Sanadhya
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, along with their applications. 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. A student will also understand the real-world constraints and several real-world attacks upon finishing this course.

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 cryptography, Number theory, Finite Fields	• Cryptology basics	2
2	Basics of Number Theory and Finite Fields	• Divisibility, Inverse Mod n • Primes and finite fields • Mathematics of RSA system • Chinese Reminder Theorem • Discrete Logarithms • Primality Testing	8

3	Symmetric Key Cryptography	• Classical Ciphers • Modern Symmetric Ciphers: Block and Stream Ciphers • Block Cipher Modes	4
4	Public Key Cryptography - encryption	• Public-key cryptography idea • Diffie-Hellman key exchange & Man-in-the-middle-attack • RSA • Security Notions in Cryptography • Elgamal encryption	4
5	Public Key Cryptography - Digital Signatures	• RSA signature scheme and its variants • Elgamal signature scheme • Schnorr signature scheme	6
6	Hash functions and Message Authentication Codes	• Properties, constructions, applications and attacks • Pseudo-random generators	7
7	Key management and Protocols	• Symmetric key distributions • Public key distributions • TLS, AEAD	5
8	Application/Advanced Topics	• Side Channel Attacks, • Authenticate data structures including	4

			hash functions, commitments, Merkle trees, blockchains and furthers. • Code based Constructions.	

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. Cryptography and Network Security, William Stallings, Pearson, 2017.
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. *Modern Cryptography: Theory and Practice* by Wenbo Mao, first edition, Pearson Education, 2004.

8. Any other remarks: None

Proposer: Angshuman Karmakar
Dated: 27/03/2026

DPGC Convener:
Dated:

The course is approved / not approved
SUGC/SPGC Chairman,
Dated: