MOOC APPROVAL REQUEST

As per KTU B.Tech Regulations 2024, Section 17

KTU Course Code:	HNCST709
KTU Course Name:	Advanced Cryptography
NPTEL Course Name:	Cryptography and Network Security
Instructor:	Prof. Sourav Mukhopadhyay
Institution:	IIT Kharagpur
Duration:	12 Weeks
Course ID:	noc26-cs18
Semester:	Jan-Apr 2026
Date:	December 02, 2025

This document contains:
1. KTU Course Syllabus (Complete)
2. NPTEL Course Details
3. Syllabus Comparison for 70% Match Verification

Submitted for approval as per R 17.5 of KTU B.Tech Regulations 2024.

SECTION A

KTU COURSE SYLLABUS

CURRICULUM

- **Total Credits: 15**
- Course Distribution:
    - Semester 4: 4 Credits
    - Semester 5: 4 Credits
    - Semester 6: 4 Credits
    - Semester 7: 3 Credits

Honours in Computer Science and Engineering											
Sl. No:	**Semester**	**Course Code**	**Course Title (Course Name)**	**Credit Structure**			**SS**	**Total Marks**		**Credits**	**Hrs./ Week**
				L	**T**	**P**		**CIA**	**ESE**		
1	**4**	HNCST409	Advanced Mathematics for Computer Science	3	1	0	5	40	60	4	4
2	**5**	HNCST509	Object Oriented Design using UML	3	1	0	5	40	60	4	4
3	**6**	HNCST609	Advanced Algorithms	3	1	0	5	40	60	4	4
4	**7**	HNCST709	Advanced Cryptography	3	0	0	4.5	40	60	3	3
Total							**20**			**15**	**15**

XX: Branch/Department Code

SYLLABUS

SEMESTER 4

SEMESTER 4

Advanced Mathematics for Computer Science

Course Code	HNCST409	**CIE Marks**	40
Teaching Hours/Week (L:T:P)	3:1:0	ESE Marks	60
Credits	4	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)	GAMAT201, PCCST201, GAMAT301	Course Type	Theory

Course Objectives:

1. To provide a rigorous mathematical foundation in number theory, graph algorithms, and information theory for the analysis of secure cryptographic systems and complex network structures.
2. To impart the theoretical and practical principles of convex optimization and Bayesian statistics required to solve parameter estimation problems and design efficient learning algorithms.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Modular arithmetic - congruence relations - modular inverses - Euclidean algorithm - Extended Euclidean algorithm - Euler's theorem - Fermat's little theorem – pseudo primes -primality testing (AKS, Miller-Rabin) - RSA cryptosystem: key generation - encryption/decryption - Galois Field (introduction and basic operations) - Hash functions (introduction)	**11**
2	Convex sets - convex functions - convex hull - identification methods - Optimization basics - local vs global minima - role of convexity - Gradient-based methods - multivariate calculus review - gradient descent algorithm - Stochastic gradient descent - mini-batch variants - learning rate concepts.	**11**
3	Bayesian paradigm - probability as belief - Bayes' theorem revisited - Conjugate priors - Beta-Binomial model - Normal-Normal model - Bayesian parameter estimation - comparison with MLE - credible intervals - Markov Chain Monte Carlo introduction - sampling from posterior distributions.	**11**
4	Graph theory review - shortest path algorithms - Dijkstra's algorithm and its improvement - Network flow - max-flow min-cut theorem - PageRank algorithm - Information theory - entropy - cross-entropy - KL divergence	**11**

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	15	10	10	40

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Solve modular arithmetic problems and congruence relations using the Extended Euclidean algorithm to execute RSA key generation, encryption, and decryption.	**K3**
CO2	Employ convex functions and gradient-based iterative methods, such as Stochastic Gradient Descent, to determine optimal solutions for multivariate objective functions.	K3
CO3	Use the Bayesian paradigm using conjugate priors to compute posterior distributions and estimate model parameters with associated credible intervals.	K3
CO4	Utilize graph algorithms to solve problems related to network routing, ranking, and understand information theoretic measures.	K3

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	**3**	**3**		**2**	**2**						**3**
CO2	**3**	**3**		**2**	**2**						**3**
CO3	**3**	**3**		**2**	**2**						**3**
CO4	**3**	**3**		**2**	**2**						**3**

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	A course in number theory and cryptography	Koblitz, Neal.	Springer Science & Business Media,	1994
2	Number theory for computing	Yan, Song Y.	Springer Science & Business Media,	2013
3	Pattern recognition and machine learning.	Christopher M. Bishop	Springer	2009
4	Convex optimization for machine learning	Changho Suh	now Publishers Inc	2022

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Machine Learning: A Probabilistic Perspective	Murphy, K. P.	MIT Press	2012
2	Python data science handbook: Essential tools for working with data	VanderPlas, Jake.	O'Reilly Media, Inc.	2016

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://onlinecourses.nptel.ac.in/noc22_cs90/preview
2	https://nptel.ac.in/courses/106101466
3	https://onlinecourses.swayam2.ac.in/imb21_mg03/preview
4	https://nptel.ac.in/courses/106106131 https://nptel.ac.in/courses/106105031

SECTION B
NPTEL COURSE DETAILS

CRYPTOGRAPHY AND NETWORK SECURITY

PROF. SOURAV MUKHOPADHYAY

Department of Computer Science and Engineering

IIT Kharagpur

INDUSTRIES APPLICABLE TO : Stratign FZE, Dubai(UAE), SAG, DRDO, ISRO, WESEE, NTRO.

COURSE OUTLINE :

The aim of this course is to introduce the student to the areas of cryptography and cryptanalysis. This course develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. Our aim is to develop a workable knowledge of the mathematics used in cryptology in this course. The course emphasizes to give a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks. A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like identity-based encryption, attribute-based encryption, functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and postquantum cryptography. The cryptanalysis part will help us understanding challenges for cybersecurity that includes network security, data security, mobile security, cloud security and endpoint security.

ABOUT INSTRUCTOR :

Sourav Mukhopadhyay is an Associate Professor, Department of Mathematics at Indian Institute of Technology Kharagpur. He has completed his B.Sc (Honours in Mathematics) in1997 from University of Calcutta, India. He has done M.Stat (in statistics) and M.Tech (in computer science) from Indian Statistical Institute, India, in 1999 and 2001 respectively. He worked with Cryptology Research Group at Indian Statistical Institute as a PhD student and received his Ph.D. degree in Computer Science from there in 2007. He was a Research Assistant at the Computer Science department of School of Computing, National University of Singapore (NUS). He visited Inria Rocquencourt, project CODES, France and worked as a post-doctoral research fellows at the School of Computer Engineering, Nanyang Technological University (NTU), Singapore. He was a post-doctoral research fellows and a part time Lecturer with School of Electronic Engineering, Dublin City University (DCU), Ireland.

COURSE PLAN :

Week 1: Introduction to cryptography, Classical Cryptosystem, Block Cipher.

Week 2: Data Encryption Standard (DES), Triple DES, Modes of Operation, Stream Cipher.

Week 3: LFSR based Stream Cipher, Mathematical background, Abstract algebra, Number Theory.

Week 4: Modular Inverse, Extended Euclid Algorithm, Fermats Little Theorem, Euler Phi-Function, Eulers theorem.

Week 5: Advanced Encryption Standard (AES), Introduction to Public Key Cryptosystem, Diffie-Hellman Key Exchange

Week 6: Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime.

Week 7: Generalized ElGamal Public Key Cryptosystem, Rabin Cryptosystem.

Week 8: Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function.

Week 9: Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS).

Week 10: Cryptanalysis, Time-Memory Trade-off Attack, Differential and Linear Cryptanalysis.

Week 11: Cryptanalysis on Stream Cipher, Modern Stream Ciphers, Shamirs secret sharing and BE, Identity-based Encryption (IBE),Attribute-based Encryption (ABE).

Week 12: Side-channel attack, The Secure Sockets Layer (SSL), Pretty Good Privacy (PGP), Introduction to Quantum Cryptography,, Blockchain, Bitcoin and Cryptocurrency.

SECTION C

SYLLABUS COMPARISON

SYLLABUS COMPARISON REPORT

KTU: HNCST709 - Advanced Cryptography
NPTEL: Cryptography and Network Security

KTU Topics	NPTEL Topics	Match
Module 1	Week 1-2	? Matched
Module 2	Week 3-4	? Matched
Module 3	Week 5-6	? Matched
Module 4	Week 7-8	? Matched
Module 5	Week 9-10	? Matched

RECOMMENDATION

This MOOC course mapping has been reviewed and is recommended for approval.

The proposed NPTEL course meets all the requirements specified in:
? R 17.1 - Approved MOOC Agency (NPTEL/SWAYAM)
? R 17.2 - Minimum 8 weeks duration
? R 17.3 - Online mode with proctored examination
? R 17.4 - At least 70% content overlap with KTU syllabus

This proposal is submitted one month before the commencement of the semester as required by R 17.5.

Verified by:

_____ _____

HoD (Department) IQAC Coordinator

_____

Principal