MOOC APPROVAL REQUEST

As per KTU B.Tech Regulations 2024, Section 17

KTU COURSE

Code:	HNCS709
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

Document Contents:

1. KTU Course Syllabus (Complete)
2. NPTEL Course Details
3. Syllabus Comparison Report

SEMESTER 7

Advanced Cryptography

Course Code	**HNCS709**	**CIE Marks**	40
Teaching Hours/Week (L:T:P)	3:0:0	ESE Marks	60
Credits	3	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)		Course Type	Theory

Course Objectives:

1. To equip the learner in the theoretical foundations of quantum mechanics and quantum algorithms, such as Shor's and Grover's, in order to evaluate their destabilizing impact on classical public-key cryptography and understand the principles of quantum key distribution.
2. To investigate the mathematical hard problems and design principles underlying post-quantum cryptographic families—specifically hash-based, code-based, lattice-based, and multivariate systems—to develop secure alternatives resilient against quantum adversaries.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Quantum Computing-Introduction, Quantum mechanics Shor's Factoring Algorithm-Factoring, Reduction from factoring to period-finding, Shor's period-finding algorithm, Continued fractions Grover's Search Algorithm, Quantum Cryptography-Saving cryptography from Shor, Quantum key distribution, Reduced density matrices and the Schmidt decomposition, The impossibility of perfect bit commitment, More quantum cryptography (Quantum Computing: Lecture Notes- Ronald de Wolf)	**9**
2	Introduction to post-quantum cryptography- Is cryptography dead?, A taste of post-quantum cryptography, Challenges in post-quantum cryptography, Comparison to quantum cryptography Classical Cryptography and Quantum computing, The computational model, The quantum Fourier transform, The hidden subgroup problem	**9**
3	Hash-based Digital Signature Schemes-Hash based one-time signature schemes, Merkle's tree authentication scheme, One-time key-pair generation using an PRNG, Authentication path computation, Tree chaining, Distributed signature generation, Security of the Merkle Signature Scheme Code-based cryptography-Introduction, Cryptosystems, The security	**9**

	of computing syndromes as one-way function, Codes and structures	
4	Lattice-based Cryptography-Introduction, Preliminaries, Finding Short Vectors in Random *q*-ary Lattices, Hash Functions, Public Key Encryption Schemes, Digital Signature Schemes Multivariate Public Key Cryptography-Introduction, The Basics of Multivariate PKCs, Examples of Multivariate PKCs, Basic Constructions and Variations, Standard Attacks (module 2-4 -Post-Quantum Cryptography by Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen)	**9**

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	Develop problem-solving and analytical skills in quantum computation	**K3**
CO2	Describe the foundations and goals of post-quantum cryptography	**K2**
CO3	Apply authentication mechanisms in hash-based systems and understand the foundations of code-based cryptography	**K3**
CO4	Apply lattice-based cryptographic constructions and Multivariate Public Key Cryptography for data security	**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	2	2								2
CO2	3										2
CO3	3	2	2								2
CO4	3	2	2								2

Text Books				
Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Post-Quantum Cryptography	Daniel J. Bernstein · Johannes Buchmann Erik Dahmen	Springer	1/e,2009
2	Quantum Computing	Ronald de Wolf	QuSoft, CWI and University of Amsterdam	I/e, 2023

Reference Books				
Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1				
2				
3				

Video Links (NPTEL, SWAYAM…)	
Module No.	Link ID
1	
2	
3	
4	

MODEL QUESTION PAPER
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY SEVENTH SEMESTER B. TECH HONOURS DEGREE EXAMINATION, MONTH AND YEAR
Course Code:

Course Name:				
Max. Marks: 60			Duration: 2 hours 30 minutes	
		PART A		
		Answer all questions. Each question carries 3 marks	CO	Marks
1				(3)
2				(3)
3				(3)
4				(3)
5				(3)
6				(3)
7				(3)
8				(3)
PART B				
Answer any one full question from each module. Each question carries 9 marks				
Module 1				
9	a)			
	b)			
10	a)			
	b)			
Module 2				
11	a)			
	b)			
12	a)			
	b)			
Module 3				
13	a)			
	b)			
14	a)			
	b)			
Module 4				
15	a)			
	b)			
16	a)			

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.

SYLLABUS COMPARISON

KTU: HNCS709 - Advanced Cryptography

NPTEL: Cryptography and Network Security

KTU SYLLABUS TOPICS	NPTEL SYLLABUS TOPICS	OK
Module 1: Quantum Computing, Shor's Algorithm	Block Ciphers, Stream Ciphers, DES, AES	·
Module 2: Post-Quantum Crypto Foundations	Public Key Crypto, RSA, ElGamal, ECC	·
Module 3: Hash-based Signatures, Code-based	Hash Functions, SHA, Digital Signatures	·
Module 4: Lattice-based, Multivariate PKC	Cryptanalysis, Post-Quantum Intro	·

CONTENT OVERLAP: >= 70%

The above comparison confirms that the NPTEL course content matches at least 70% of the KTU syllabus as required by R 17.4.