

Ramrao Adik Institute of Technology, Nerul, Navi Mumbai Department of Computer Science and Engineering (AI-ML)

		Theory Hrs	Practical Hrs	Tutorial Hrs	Theory Credit	Practical/Oral Credit	Tutorial Credits	Total Credits
CAC601	Cryptog raphy & Network Security	03	-	-	03	-	-	03

Subject Code	Subject Name	Examination Scheme								
		Theory Marks				Term Work	Practical & Oral	Oral	Total	
		In-Sem Evaluations End								
		IA1	IA2	Avg. IA	Mid Sem Exam	Sem Exam				
CAC601	Cryptography & Network Security	20	20	20	20	60				100

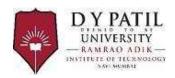
Course Objectives:

- 1. To understand concepts of classical encryption techniques, modular arithmetic and number theory.
- 2. To explore the fundamental aspects of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.
- 3. To explore various authentication protocols, PKI standards and various secure communication standards.

Course Outcomes: At the end of the course learner will able to

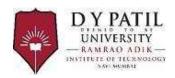
- 1. Understand the basic fundamentals of cryptographic techniques along with arithmetic required for cryptography.
- 2. Apply the different cryptographic algorithms to ensure confidentiality of the data.
- 3. Appraise the fundamental aspects of key management techniques.
- 4. Apply appropriate cryptographic hash functions to maintain integrity of data.
- 5. Apply different digital signature algorithms to achieve authentication and design secure applications.
- 6. Perceive network security concepts and various network security protocols and also analyze different network attacks.

Prerequisites: Engineering Mathematics, Computer Networks



Ramrao Adik Institute of Technology, Nerul, Navi Mumbai Department of Computer Science and Engineering (AI-ML)

Sr. No.	Module	Detailed Content	Hours	CO Mapping
1	Introduction to Cryptography	Security Goals, Attacks, Services and Mechanisms. Integer Arithmetic and Modular Arithmetic: Euclidean Algorithm Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's theorem Classical Encryption techniques, Symmetric cipher model, cryptanalysis Mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, Transposition techniques: keyed and keyless transposition ciphers	08	CO1
2	Symmetric and Asymmetric key Cryptography	Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA Cryptosystem, The knapsack cryptosystem, ElGamal cryptosystem, Elliptic curve cryptosystem	10	CO2
3	Key Management	Symmetric Key Distribution: KDC, Needham-schroeder protocol. Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman, Public key Distribution: Digital Certificate: X.509, PKI	06	CO3
4	Cryptographic Hash Functions	Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.	04	CO4
5	Authentication Protocols & Digital Signature	User Authentication, Entity Authentication: Password Based, Challenge Response Based Digital Signature, Attacks on Digital Signature, Digital Signature Scheme: RSA, ElGamal, Elliptic curve, Schnorr	04	CO5
6	Network Security and Applications	Network security basics: TCP/IP vulnerabilities (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing Denial of Service, Internet Security Protocols: SSL, IPSEC. Email Security: PGP System security: IDS, Firewalls, malicious Programs: Worms and Viruses, SQL injection	07	CO6



Ramrao Adik Institute of Technology, Nerul, Navi Mumbai Department of Computer Science and Engineering (AI-ML)

Text Books:

- 1. Behrouz A. Ferouzan, —Cryptography & Network Security, Tata Mc Graw Hill
- 2. William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
- 3. Bernard Menezes, —Cryptography & Network Security, Cengage Learning.
- 4. Network Security Bible, Eric Cole, Second Edition, Wiley.

Reference Books:

- 1. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley.
- 2. Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

Evaluation Scheme:

In-Semester Assessment:

Assessment consists of two Internal Assessments (IA1, IA2) out of which; one should be compulsory class test (on minimum 02 Modules) and the other is a class test / assignment on case studies / course project.

Mid Semester Examination (MSE) will be based on 40-50% of the syllabus.

End-Semester Examination:

- Question paper will comprise of full syllabus.
- In the question paper, weightage of marks will be proportional to the total number of lecture hours as mentioned in the syllabus