

### Cryptography and Information Security

<b>Course Code</b>	20CS4501B	<b>Year</b>	III	<b>Semester</b>	I
<b>Course Category</b>	PEC	<b>Branch</b>	CSE	<b>Course Type</b>	Theory
<b>Credits</b>	3	<b>L-T-P</b>	3-0-0	<b>Prerequisites</b>	-
<b>Continuous Evaluation :</b>	30	<b>Semester End Evaluation:</b>	70	<b>Total Marks:</b>	100

#### Course Outcomes

Upon successful completion of the course, the student will be able to

<b>CO1</b>	Understand the Basic concepts of security over the network.	<b>L2</b>
<b>CO2</b>	Apply various Key Management Techniques for secure key sharing.	<b>L3</b>
<b>CO3</b>	Analyze encryption algorithms and security protocols for their strengths and weaknesses	<b>L3</b>

#### Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
<b>CO1</b>	√													
<b>CO2</b>						√	√							√
<b>CO3</b>						√	√		√	√				√

Syllabus		Mapped CO
Unit No.	Contents	
I	<b>Security Concepts:</b> The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. <b>Classical Encryption Techniques:</b> Substitution Techniques and Transposition Techniques.	CO1
II	<b>Block Ciphers and the Data Encryption Standard:</b> Traditional Block Cipher Structure, The Data Encryption Standard, Advanced Encryption Standard, Block Cipher operation.	CO1, CO3
III	<b>Public key cryptography:</b> Principles, RSA, Diffie-Hellman key exchange algorithm. <b>Cryptographic Hash Functions:</b> Secure Hash Algorithm (SHA-512), MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC.	CO1, CO3
IV	<b>Key Management and Distribution:</b> Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates. Public-Key Infrastructure, Kerberos	CO1, CO2
V	<b>Email Security:</b> S/MIME, Pretty Good Privacy. <b>IP Security:</b> IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange.	CO1, CO3

### Learning Resources

#### Text Books

1. William Stallings. Cryptography and Network Security – Principles and Practice, Seventh edition, Pearson Education, 2017.

#### References

1. Cryptography and Network Security, Forouzan and Mukhopadhyay, Third edition, 2015, Mc Graw Hill.
2. Cryptography and Network Security, Atul Kahate, Third edition, Mc Graw Hill, 2013.

#### e-Resources & other digital material

1. <http://nptel.ac.in/courses/106105031/lecture>, Dr. Debdeep Mukhopadhyay, IIT Kharagpur
2. <https://www.coursera.org/learn/information-security-data>
3. <https://www.coursera.org/learn/number-theory-cryptography>