CRYPTOGRAPHY

(Honors)

Course Code		**Year**	II	**Semester**	II
Course Category	HONORS	**Branch**	IT	**Course Type**	Theory
Credits	4	**L-T-P**	4-0-0	**Prerequisites**	Computer Networks, Number Theory
Continuous Internal Evaluation :	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon Successful completion of course, the student will be able to		
CO1	Understand various attacks , types of cryptography, cryptographic data integrity algorithms and basics of Email and IP security	L2
CO2	Identify various cryptographic techniques	L3
CO3	Interpret various cryptographic data integrity algorithms	L2
CO4	Apply the field of cryptography while designing security applications.	L3

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations (3:High, 2: Medium, 1:Low)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	3												2	2
CO2		3											2	2
CO3	3												2	2
CO4	3												2	2

Syllabus

Unit No	**Contents**	**Mapped CO**
I	**Security Fundamentals:** Security Attacks, Security Services, Security Mechanisms, A model for Network security.	**CO1**
II	**Secret Key Cryptography:** Symmetric cipher model, Block and Stream ciphers, Data Encryption Standard (DES), Strength of DES, Block cipher design principles and modes of operation, Multiple encryption and Triple DES, AES Structure.	**CO1, CO2, CO4**
III	**Public-key Cryptography:** Principles of public-key crypto systems, RSA algorithm, Diffie-Hellman key exchange, Introduction to elliptic curve cryptography.	**CO1, CO2, CO4**
IV	**Hash Functions and Digital Signatures:** Cryptographic hash functions, Applications of cryptographic hash functions, secure hash algorithm, authentication algorithms- HMAC, Digital signatures, Digital Signature algorithm.	**CO1, CO3, CO4**
V	**E-mail Security and IP Security:** E-mail Security: PGP, S/MIME. IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload.	**CO1, CO4**

Learning Resources

Text Books

1. Cryptography and Network Security Principles and practice by W. Stallings 7th edition Pearson Education Asia 2017

2. Cryptography and Network Security by Behrouz A. Forouzan and Debdeep Mukhopadhyay 2nd edition Tata McGraw Hill 2013

References

1. "Cryptography: Theory and Practice" Stinson. D. 3rd edition Chapman & Hall/CRC 2012
2. "Cryptography and Network Security" Atul Kahate Tata McGraw-Hill 2003

E-Recourses and other Digital Material

1. https://nptel.ac.in/courses/106106221
2. http://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf