	CRYPTOGRAPHY AND NETWORK SECURITY	L	T	P	C
		3	0	0	3

PREREQUISITE :	
	Data Communications and Network Security

COURSE OBJECTIVES:

1. To understand the basics of cryptography
2. To learn to find the vulnerabilities in programs and to overcome them
3. To know the different kinds of security threats in networks and its solution
4. To know the different kinds of security threats in databases and solutions available
5. To learn about the models and standards for security.

UNIT I	**ELEMENTARY CRYPTOGRAPHY**	**09 Hours**

Terminology and Background – Substitution Ciphers – Transpositions – Making Good Encryption Algorithms- Data Encryption Standard- AES Encryption Algorithm – Public Key Encryption –Cryptographic Hash Functions – Key Exchange – Digital Signatures – Certificates

UNIT II	**PROGRAM SECURITY**	**09 Hours**

Secure programs – Non-malicious Program Errors – Viruses – Targeted Malicious code – Controls Against Program Threat – Control of Access to General Objects – User Authentication – Good Coding Practices – Open Web Application Security Project Flaws – Common Weakness Enumeration Most Dangerous Software Errors

UNIT III	**SECURITY IN NETWORKS**	**09 Hours**

Threats in networks – Encryption – Virtual Private Networks – PKI – SSH – SSL – IPSec – Content Integrity – Access Controls – Wireless Security – Honeypots – Traffic Flow Security – Firewalls –Intrusion Detection Systems – Secure e-mail.

UNIT IV	**SECURITY IN DATABASES**	**09 Hours**

Security requirements of database systems – Reliability and Integrity in databases –Redundancy –Recovery – Concurrency/ Consistency – Monitors – Sensitive Data – Types of disclosures –
Inference-finding and confirming sql injection

UNIT V	**SECURITY MODELS AND STANDARDS**	**09 Hours**

Secure SDLC – Secure Application Testing – Security architecture models – Trusted Computing Base– Bell-LaPadula Confidentiality Model – Biba Integrity Model – Graham-Denning Access Control Model – Harrison-Ruzzo-Ulman Model – Secure Frameworks – COSO – CobiT – Compliances – PCI DSS – Security Standards - ISO 27000 family of standards – NIST.

TOTAL: 45 HOURS

FURTHER READING:

1. Challenge –Handshake Authentication Protocol (CHAP)

COURSE OUTCOMES:

On the successful completion of the course, students will be able to

CO1:	Apply cryptographic algorithms for encrypting and decryption for secure data transmission
CO2:	Understand the importance of Digital signature for secure e-documents exchange
CO3:	Understand the program threats and apply good programming practice
CO4:	Get the knowledge about the security services available for internet and web applications
CO5:	Gain the knowledge of security models and published standards

REFERENCES:

1. Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing”, Fourth Edition, Pearson Education, 2007
2. William Stallings, “Cryptography and Network Security : Principles and Practices”, Fifth Edition,Prentice Hall, 2010.
3. Michael Howard, David LeBlanc, John Viega, “24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them”, First Edition, McGrawHill Osborne Media, 2009.
4. Michael Whitman, Herbert J. Mattord, “Management of Information Security”, Third Edition, Course Technology, 2010.
5. Matt Bishop, “Computer Security: Art and Science”, First Edition, Addison-6. Wesley, 2002
6. https://www.tutorialspoint.com/cryptography/index.htm
7. https://nptel.ac.in/courses/106/105/106105031/