Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous Institute Affiliated to University of Mumbai)

Course Code	Course Name	Teaching Scheme (Hrs/week)			Credits Assigned			
		L	T	P	L	T	P	Total
CPC702	Cryptography and System Security	4	-	--	4	-	--	4
		Examination Scheme						
		ISE		MSE		ESE		
		10		30		100 (60% Weightage)		

Pre-requisite Course Codes		-
At end of successful completion of this course, student will be able to		
Course Outcomes	CO1	Understand the principles and practices of cryptographic techniques.
	CO2	Understand a variety of generic security threats and vulnerabilities, and identify & analyze particular security problems for given application.
	CO3	Appreciate the application of security techniques and technologies in solving real-life security problems in practical systems.
	CO4	Design security protocols and methods to solve the specific security problems.
	CO5	Familiar with current research issues and directions of security.

Module No.	Topics	Ref.	Hrs.
1	**Introduction** Security Attacks, Security Goals, Computer criminals, Methods ofdefense, Security Services, Security Mechanisms	1-6	**06**
2	**Basics of Cryptography** Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties- Confusion, Diffusion, Block and Stream Ciphers.	1-6	**06**
3	**Secret Key Cryptography** Data Encryption Standard(DES), Strength of DES, Block Cipher Design Principles and Modes of Operations, Triple DES, International Data Encryption algorithm, Blowfish, CAST-128.	1-6	**06**
4	**Public Key Cryptography** Principles of Public Key Cryptosystems, RSA Algorithm, Diffie-Hellman Key Exchange	1-6	**04**
5	**Cryptographic Hash Functions** Applications of Cryptographic Hash Functions, Secure Hash Algorithm, Message Authentication Codes – Message Authentication Requirements and Functions, HMAC, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards.	1-6	**06**
6	**Authentication Applications** Kerberos, Key Management and Distribution, X.509 Directory	1-6	**06**

	Authentication service, Public Key Infrastructure, Electronic Mail Security: Pretty Good Privacy, S/MIME.		
7	**Program Security, Operating System Security, Database Security, IDS and Firewalls** Secure programs, Non-malicious Program Errors, Malicious Software–Types, Viruses, Virus Countermeasures, Worms, Targeted Malicious Code, Controls against Program Threats, Memory and Address protection, File Protection Mechanism, User Authentication, Security Requirement, Reliability and Integrity, Sensitive data, Inference, Multilevel Databases Intruders, Intrusion Detection, Password Management, Firewalls-Characteristics, Types of Firewalls, Placement of Firewalls, Firewall Configuration, Trusted systems.	1-6	**08**
8	**IP Security** Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining security Associations, Internet Key Exchange, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Electronic Payment, Non-cryptographic protocol Vulnerabilities, DoS, DDoS, Session Hijacking and Spoofing, Software Vulnerabilities-Phishing, Buffer Overflow, Format String Attacks, SQL Injection.	1-6	**06**
		Total	**48**

References:

[1] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson, 5th edition.

[2] Bernard Menezes, "Network Security and Cryptography", Cengage Learning, 2nd edition.

[3] Behrouz A Fourouzan, Debdeep Mukhopadhyay, "Cryptography and Network", TMH, 2nd edition.

[4] Behrouz A. Forouzan,"Cryptography and Network Security", TMH

[5] Charles P. Pfleeger,"Security in Computing", Pearson Education.

[6] Matt Bishop, "Computer Security Art and Science", Addison-Wesley.