GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering
Subject Code: 3726107
Semester – II
Subject Name: Network Security and Cryptography

Type of course: Elective

Prerequisite: NA

Rationale:

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Content:

Sr. No.	Content	Total Hrs
1	Security - Need, security services, Attacks, OSI Security Architecture, one time passwords, Model for Network security, Classical Encryption Techniques like substitution ciphers, Transposition ciphers, Cryptanalysis of Classical Encryption Techniques	
2	Number Theory - Introduction, Fermat's and Euler's Theorem, The Chinese Remainder Theorem, Euclidean Algorithm, Extended Euclidean Algorithm, and Modular Arithmetic	
3	Private-Key (Symmetric) Cryptography - Block Ciphers, Stream Ciphers, RC4 Stream cipher, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES, RC5, IDEA, Linear and Differential Cryptanalysis.	
4	Public-Key (Asymmetric) Cryptography - RSA, Key Distribution and Management,Diffie-Hellman Key Exchange, Elliptic Curve Cryptography, Message Authentication Code, hash functions, message digest algorithms: MD4 MD5, Secure Hash algorithm, RIPEMD-160, HMAC	
5	Authentication - IP and Web Security Digital Signatures, Digital Signature Standards, Authentication Protocols, Kerberos, IP security Architecture, Encapsulating Security Payload, Key Management, Web Security Considerations, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction.	
6	System Security - Intruders, Intrusion Detection, Password Management, Worms, viruses, Trojans, Virus Countermeasures, Firewalls, Firewall Design Principles, Trusted Systems.	

Reference Books:

1. William Stallings, "Cryptography and Network Security, Principles and Practices", Pearson Education, 3rd Edition.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security, Private Communication in a Public World", Prentice Hall, 2nd Edition
3. Christopher M. King, ErtemOsmanoglu, Curtis Dalton, "Security Architecture, Design Deployment and Operations", RSA Pres,

4. Stephen Northcutt, LenyZeltser, Scott Winters, Karen Kent, and Ronald W. Ritchey, "Inside Network Perimeter Security", Pearson Education, 2nd Edition
5. Richard Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response", William Pollock Publisher, 2013.

Course Outcome:

After learning the course the students should be able to:

Sr. No.	CO statement	Marks % weightage
CO-1	Identify and utilize different forms of cryptography techniques.	
CO-2	Incorporate authentication and security in the network applications	
CO-3	Distinguish among different types of threats to the system and handle the same.	