C. U. SHAH UNIVERSITY – WADHWAN CITY

FACULTY OF TECHNOLOGY AND ENGINEERING
DEPARTMENT OF INFORMATION TECHNOLOGY
B. TECH. SEMESTER: - VI

Subject Name: Cryptography and Network Security (CNS)
Subject Code: 4TE06CNS1

Teaching & Evaluation Scheme:-

Subject Code	Subject Name	Teaching Scheme (Hours)				Credits	Evaluation Scheme							
							Theory				Practical (Marks)			Total
							Sessional Exam		University Exam		Internal		University	
		Th	Tu	Pr	Total		Marks	Hours	Marks	Hours	Pr/Viva	TW	Pr	
4TE06CNS1	Cryptography and Network Security (CNS)	4	0	2	6	5	30	1.5	70	3.0	-	20	30	150

Objectives:

- To understand the basics of Cryptography like Symmetric and Asymmetric algorithms, Hash algorithms, Digital Signature
- To know the legal, ethical and professional issues in Information Security.
- To become aware of various standards in this area.

Prerequisites:

- Knowledge of Computer Network and Internet.

Course outline:

Sr. No.	Course Contents	Total Hrs.
1	**Fundamentals:** Security Attacks, Services, Mechanisms, Network Security Model, Conventional Encryption Model, Types of Cryptanalytic Attacks, Steganography.	6
2	**Conventional Cryptography:** Classical Encryption Techniques, Simplified DES, Block Cipher Principles, Feistel Cipher, Data Encryption Standard, Block Cipher Design Principles And Modes Of Operation, Triple DES, International Data Encryption Algorithm, Blowfish, RC5, Characteristics Of Advanced Symmetrical Block Ciphers, Key Distribution, Random Number Generation.	12
3	**Public Key Cryptography:** Principles Of Public-Key Cryptography, Key Management, Prime and Relative Prime Numbers, Euler's Theorem, Euclid's Theorem, Diffie-Hellman Key Exchange, Elliptic Curve Encryption/Decryption, RSA Algorithm, Security Attacks on RSA.	10

4	**Message Authentication And Hash Functions:** Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Security of Hash Functions And MACs, MD5, Secure Hash Algorithm, HMAC.	**8**
5	**Digital Signature and Authentication Protocols:** Digital Signatures, Authentication Protocols, Digital Signature Standard, Authentication Applications like Kerberos, X.509 Authentication Service.	**8**
6	**Network Security:** **Email Security:** Overview, Pretty Good Privacy, S/MIME, **IP Security:** Overview, Architecture, Authentication Header, Encapsulation Security Payload, **Web Security:** Web Security Requirements, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction.	**10**
7	**System Security:** Intruders, Viruses and related Threats, Firewall Design Principles, Trusted Systems.	**6**
	TOTAL:	**60**

Learning Outcomes:

At the end of this subject students will be well familiar with:

- Different security algorithms used in real time applications.
- Technological aspects of Information Security.

Books Recommended:

1. Cryptography and Network Security: Principles and Practice, Fourth Edition, **William Stallings**, Pearson
2. Cryptography and Network Security, Second Edition, **Atul Kahate**, Tata McGraw-Hill
3. Cryptography and Network Security, Second Edition, **Behrouz A. Forouzan, Debdeep Mukhopadhyay**, Tata McGraw-Hill.