# C. U. SHAH UNIVERSITY – WADHWAN CITY

## FACULTY OF TECHNOLOGY AND ENGINEERING DEPARTMENT OF COMPUTER ENGINEERING M. TECH. SEMESTER: - II

**SUBJECT NAME:** **Advanced Cryptography and Network Security (ANS)**
**SUBJECT CODE:** **5TE02ANS1**

---

### Teaching & Evaluation Scheme: -

| Subject Code | Subject Name | Teaching Scheme (Hours) | | | | Credits | Evaluation Scheme | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Th | Tu | Pr | Total | | Theory | | | | Practical (Marks) | | | Total |
| | | | | | | | Sessional Exam | | University Exam | | Internal | | University | |
| | | | | | | | Marks | Hours | Marks | Hours | Pr/Viva | TW | Pr | |
| 5TE02ANS1 | Advanced Cryptography and Network Security | 4 | 0 | 2 | 6 | 5 | 30 | 1.5 | 70 | 3.0 | - | 20 | 30 | 150 |

### Objectives:

To understand basics of Cryptography.
To understand Network Security concepts.

### Prerequisites:

Basic Knowledge of Networks/System

### Course outline:

| Sr. No. | Course Contents |
|---|---|
| 1 | **Introduction:**<br>Threats,Vulnerabilities,Attacks,Integrity,Confidentiality,Anonymity,Authentication, Authorization, Non-repudiation, Data Security and Database Security |
| 2 | **Secret Key Cryptography:**<br>DES, Triple DES, AES, Key Distribution, Attacks |
| 3 | **Public Key Cryptography:**<br>RSA, ECC, Key Exchange, Attacks. |
| 4 | **Integrity, Authentication and Non-Repudiation:**<br>Hash Functions, Message Authentication Code, Digital Signature |
| 5 | **Public Key Infrastructure:**<br>Digital Certificates, Certification Authorities. |
| 6 | **Protocols:**<br>Basic Authentication Protocols, Attacks, Needham Schroeder Protocol, Kerberos, Network Security with IP Security, Web Security using SSL, Ecash and Secure Electronic Transaction |
| 7 | **System Security using Firewalls and VPNs** |

| | |
|---|---|
| 8 | **Worms and Viruses** |
| 9 | **Miscellaneous:**<br>Smart Cards and security, Zero knowledge protocols, Enterprise Application Security, Biometric Authentication, Database Access Control, Security and Privacy Issues in RFIDs |

## Learning Outcomes:

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

- Different Cryptography algorithms
- Network Security Protocols

## Books Recommended:

1. Cryptography and Network Security, 4th Edition by **William Stallings,** Pearson Education India (2006)
2. Security in Computing, **Pfleeger and Pfleeger**; 3rd Edition, PHI
3. Computer Security: Art and Science, **Bishop**; Pearson Edition
4. Computer Security, 3rd Edition **Dieter Gollmall**; Willey Publication(2010)
5. Network Security, 2nd Edition by **Kaufman**; Pearson Edition (2002)