# UNIVERSITY OF MADRAS

BACHELOR OF COMPUTER APPLICATIONS (BCA)
DEGREE PROGRAMME
SYLLABUS WITH EFFECT FROM 2023-2024

**Year: III** **Semester: VI**

| **Network Security**<br><br>Common for B.C.A. , B.Sc.-SA | **320E6F** |
|---|---|
| **Credits 3** | **Lecture Hours:5 per week** |

**Learning Objectives:** (for teachers: what they have to do in the class/lab/field)

- To study the number theory used for network security
- To understand the design concept of cryptography and authentication
- To develop experiments on algorithm used for security

**Course Outcomes:** (for students: To know what they are going to learn)

1. Identify the security issues in the network and resolve it.
2. Analyse the vulnerabilities in any computing system and hence be able to design a security solution.
3. Evaluate security mechanisms using rigorous approaches by key ciphers and Hash functions.
4. Demonstrate various network security applications, IPSec, Firewall, IDS, Web Security, Email Security and Malicious software etc

| **Units** | **Contents** |
|---|---|
| **I** | Model of network security – Security attacks, services and attacks –OSI security architecture – Classical encryption techniques – SDES – Block cipher PrinciplesDES – Strength of DES – Block cipher designprinciples–Block cipher mode of operation – Evaluation criteria for AES – RC4 - Differential and linear cryptanalysis – Placement of encryption function – traffic confidentiality. |
| **II** | Number Theory – Prime number – Modular arithmetic – Euclid's algorithm - Fermet's and Euler's theorem – Primality –Chineseremaindertheorem– Discrete logarithm – Public key cryptography and RSA – Key distribution – Key management – Diffie Hellman key exchange – Elliptic curve cryptography. |
| **III** | Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC– SHA - HMAC – CMAC - Digital signature and authentication protocols – DSS. |
| **IV** | Authentication applications – Kerberos – X.509 Authentication services - E- mail security – IP security - Web security |
| **V** | Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security |

**Learning Resources:**

**Recommended Texts**

1. William Stallings, "Cryptography & Network Security", Pearson Education, Fourth Edition 2010.

**Reference Books**

1. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security, Private communication in public world", PHI Second Edition, 2002.
2. Bruce Schneier, Neils Ferguson, "Practical Cryptography", Wiley Dreamtech India Pvt Ltd, First Edition, 2003.
3. Douglas R Simson "Cryptography – Theory and practice", CRC Press, First Edition, 1995.