

Semester VIII

BCA 8011:Network Security & Cryptography (Theory)

Course Learning Outcomes:

After undergoing the course, Students will be able :

- To understand basics of Cryptography and Network Security.
- To secure a message over insecure channel by various means.
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
- To understand various protocols for network security to protect against the threats in the networks.

Credit: 04

60 Hours

Unit I: Introduction to security, brief history of cryptography, understanding attacks, services, mechanisms, security attacks, security services, model for network security, internet standards, Basic principles of good cryptosystems, Modular arithmetic and GF (2), substitution and transposition ciphers, Stream ciphers, Pseudo Random Number generators. [6Hrs]

Unit II: Symmetric block ciphers, DES, Gallois field, polynomial arithmetic, AES, Principles of S Box design, Block cipher design principles, Other Block ciphers. [6Hrs]

Unit III: Introduction to public key cryptography, Number theoretic foundations, public key cryptography principles, RSA encryption system, primality testing, Number theoretic algorithms, Attacks on RSA. [12 Hrs]

Unit IV: Discrete Logarithm and Diffie-Hellman Key exchange, ElGamal system, Digital Signature, RSA and ElGamal based Digital signature, DSA, different attacks on digital signatures. [12 Hrs]

Unit V: Secure hash functions, Understanding Collisions, Secure Hash Algorithms, SHA, HMAC, Key establishment and key management, Digital Certificates. [6Hrs]

Unit VI: Advanced topics on cryptography: Integer factorization, Strong primes, distribution of Primes, Lattice based cryptography, Introduction to Elliptic curves, Introduction to Elliptic curve-based cryptography, Secret Sharing, Zero Knowledge Proof. [10Hrs]

Unit VII: Authentication, e mail security, Kerberos, x.509 directory authentication services, PGP, S/MIME. Overview of IP security, IP security architecture,

authentication header, encapsulating security pay load, combining security associations.
[4 Hrs]

Unit VIII: Introduction to web security, web security requirements, SSL & transport layer security, SET network management security. Basics of system security, intruders, viruses-related threats, firewalls, design principles, trusted systems. [4Hrs]

BCA 8011: Network Security & Cryptography (Practical)

Credit: 02

60 Hours

1. Implement [RSA Algorithm](#).
 2. Implement Elliptic curve-based cryptography
 3. Implement SSL/TLS for secure browser communication using [OpenSSL](#)
 4. Implement [Digital Signature Algorithm \(DSA\)](#) .
 5. Implement SSL/TLS for secure browser communication using [OpenSSL](#)
 6. Setting up Firewall rules using [iptables](#) in Linux
 7. Implement [Secure Hash Algorithm](#) implementation
 8. Implement Primality testing using Fermat's theorem.
 9. Implement Miller-Rabin Test.
 10. Find inverse of an element in a ring using EEA.
 11. Implement Modular Arithmetic and Polynomial Arithmetic.
-

BCA 8021: Operations Research (Theory)

Course Learning Outcomes:

- Explain the historical development, nature, and scope of Operations Research.
- Formulate complex business scenarios into mathematical Linear Programming Models and solve them using **Graphical** and **Simplex** methods to find optimal solutions.
- Apply **Transportation** and **Assignment** algorithms to minimize costs and maximize efficiency in supply chain and resource allocation scenarios.
- Analyze competitive situations using **Game Theory** and apply **Decision Theory**
- Construct and analyze project networks using **PERT** and **CPM**.

Credit: 03

45 Hours

UNIT – I: Introduction: Historical Development: Definitions of OR; Nature and scope of Study; Phases of OR; Classification of OR models; Methodology of OR. **5 LH**

UNIT – II: Linear programming: Assumptions, Basic concepts; LP Formulation Graphical Solution – Feasible Region, Optimum Solution, special cases (unbounded solutions, infeasible solution and Alternative optima). **12 LH**

UNIT - III: Standard Form, Canonical form and Simplex method – maximization case, minimization case; Big – M method. **8 LH**

UNIT- IV: Transportation Problem: Transportation tableau, Mathematical Form, Methods for Finding Initial basic Feasible Solution – North West Corner Rule, Least Cost Method, VAM; Test for Optimality – MODI Method. **10 LH**

UNIT- V: Assignment Problem: Mathematical Statement of Problem, Comparison with Transportation Problem; Solution of Assignment Problem – Hungarian Methods. **10 LH**

UNIT- VI: Game Theory: Introduction; Two – person zero – some Games; Games with saddle Point – Pure Strategies; Rules of Dominances. **8 LH**

UNIT- VII: Decision Theory: Steps in Decision Theory Approach; Types of Decision-Making Environments; Decision Making Under Risk – Expected Monetary Value, Expected Opportunity loss; Decision Making Under Uncertainty – Criterion of optimism, Criterion of Pessimism, Laplace Criterion, Criterion on Regret. **8 LH**

UNIT- VIII: Network Analysis (PERT and CPM) : Introduction; Network Construction; Critical Path Analysis – Forward Pass, Backward Pass and Float of an Activity and Event, Critical Path, Estimation of Project Completion Time. **10 LH**

References Book :

1. Operations Research; Theory and Applications – J. K. Sharma; Macmillan.
2. Operation Research – P. K. Gupta and D. S. Hira; S. Chand.
3. Quantitative Technique in Management – N. D. Vhora; Tata McGraw Hill.
4. Operation Research – K. Swarup, P. K. Gupta and M. Mohan; Sultan Chand.
5. Operation Research: An introduction – H. A. Taha; Macmillan.

BCA 8021: Operations Research (Tutorial)**Credit:1****15 Hour****Tutorial based on concepts listed in theory.**