Batch 2024-25

Syllabus

2nd Semester

M.Sc. (Computer Science)

M.Sc(CS)

Semester 2

241/CS/CC201

CRYPTOGRAPHY AND NETWORK SECURITY

Semester	2			
Course code	CC-A04			
Category	Core Course(s)			
Course title	Cryptography and Network Security			
Course ID	241/CS/CC201			
Scheme and Credits	L	T	P	Credits
	3	0	2	4
Theory Internal	25 marks			
Theory External	50 marks			
Practical Internal	5 marks			
Practical External	20 marks			
Total	100 marks			
Duration of Exam	3 hrs			

Note: *The examiner will set nine questions in total. Question one will have seven parts from all units and the marks of first question will be of 20% of total marks of Question Paper and the remaining eight questions to be set by taking two questions from each unit and the marks of each question from Question no.2 to 9 will be of 20% of total marks of Question paper. The students have to attempt five questions in total, the first being compulsory and selecting one from each unit.*

COURSE OUTCOMES:

At the end of this course, students will demonstrate the ability to

CO1: Discover all the Information Security Goals, Services & Mechanism for Network Security & necessity of Mathematics in designing crypto algorithms.

CO2: Develop and design various kinds of Symmetric Key crypto algorithms and to cryptanalyze them.

CO3: Construct and design various kinds of Asymmetric key crypto algorithms and Mathematics required for designing.

CO4: Analyze the integrity of information transmitted & to generate digital signatures.

CO5: Predict and apply the knowledge and skills obtained to design & understand latest cryptographic protocols used for securing information in networks or in storage.

UNIT-I

INTRODUCTION TO INFORMATION SECURITY & CRYPTOGRAPHY: What is Information Security, Need for security, Principles of Security, Threats, Types of Attacks, Services & Mechanisms, Mathematics of Cryptography: Integer Arithmetic, Modular Arithmetic, Matrices, Linear Congruence.

UNIT-II

SYMMETRIC KEY CIPHERS: Traditional Symmetric –Key Cipher design and analysis-Different Substitution ciphers & Transposition ciphers, Basic Principles of designing Stream cipher & Block cipher. Mathematics of Symmetric-Key Cryptography-Algebraic Structures, GF (2n) Fields.

Modern Symmetric key Ciphers- Block Ciphers Design & Analysis - Data encryption Standard (DES), Advanced Encryption Standard (AES) Stream Ciphers Design & Analysis-LFSR based, RC4, A5/1.

UNIT-III

ASYMMETRIC KEY CIPHERS, HASH FUNCTIONS AND DIGITAL SIGNATURES: Mathematics of Asymmetric-Key Cryptography, Asymmetric key Ciphers, Hash Functions and MAC, Introduction to Digital Signatures.

UNIT-IV

NETWORK SECURITY: Network Security: Security at application layer – PGP & S/MIME, Key distribution Centre, Diffie- Hellman Key Exchange.

TEXT AND REFERENCE BOOKS:

1. Cryptography and Network Security 7th Edition, William Stallings
2. Cryptography and Network Security, 4rd edition, Forouzan & Mukopadhyay, TMH.
3. Information Security & Cryptography-Cryptography Made Simple, Nigel P Smart, Springer Verlag,2016.
4. Cryptography & Network Security, 2nd Edition, Atul Kahate. McGrawHill.

CRYPTOGRAPHY AND NETWORK SECURITY LAB

List of Subject related Experiments:

1. Program to find GCD of any two numbers a and b modn by Generalized Euclidean Algorithm
2. Program to encrypt and decrypt by Ceaser Cipher
3. Program to Encrypt and Decrypt by Affine Cipher
4. Program to encrypt plaintext by Playfair Cipher
5. Program to generate addition and multiplication table for GF(22) Field
6. Program for key expansion algorithm of DES
7. Program to implement 4*4 S-box and perform two functionalities:
   a.) Check given table of S-box and inverse S-box are invertible to each other.
   b.) Ask the user to enter input to be given in S-box and return its output.
8. Program to implement encryption and decryption of RSA algorithm.

241/CS/CC202

PROGRAMMING IN JAVA

Semester	2			
Course code	CC-A05			
Category	Core Course(s)			
Course title	Programming in Java			
Course ID	241/CS/CC202			
Scheme and Credits	L	T	P	Credits
	3	0	2	4
Theory Internal	25 marks			
Theory External	50 marks			
Practical Internal	5 marks			
Practical External	20 marks			
Total	100 marks			
Duration of Exam	3 hrs			

Note:*The examiner will set nine questions in total. Question one will have seven parts from all units and the marks of first question will be of 20% of total marks of Question Paper and the remaining eight questions to be set by taking two questions from each unit and the marks of each question from Question no.2 to 9 will be of 20% of total marks of Question paper. The students have to attempt five questions in total, the first being compulsory and selecting one from each unit.*

COURSEOUTCOMES:

At the end of this course, students will demonstrate the ability to

CO1: Identify classes, objects, members of a class and relationships among them for a specific problem.

CO2: Understand and demonstrate the concepts of garbage collection, polymorphism, inheritance etc.

CO3: Do numeric (algebraic) and string-based computation.

CO4: Understand and implement modularity as well as basic error-handling techniques.

CO5: Develop, design and implement small multithreaded programs using Java language.

CO6: Apply appropriate problem-solving strategies for the implementation of small/medium scale Java applications.

UNIT-I

Introduction to Java: Evolution of Java, Object Oriented Programming Structure, Overview and characteristics of Java, Java program Compilation and Execution Process, Organization of the

Java Virtual Machine, Platform Independency & Portability, Security, Relation b/w JVM, JRE and JDK, Introduction to JAR format, Naming Conventions, Data types & Type casting, operators, Arrays.

UNIT-II

Object-Oriented Concepts: Class and objects—fundamentals of classes, creating objects, assigning object reference variables, introducing methods, static methods, constructors, constructor overloading, this keyword, method overloading, garbage collection, and the finalize() method.

Inheritance and Polymorphism: Basics of inheritance, access control, multilevel inheritance, method overriding, abstract classes, polymorphism, and the final keyword.

UNIT-III

Packages: Defining packages, setting CLASSPATH, package naming, accessibility of packages, and using package members.

Interfaces: Implementing interfaces, differences between interfaces and abstract classes, and using extends and implements together.

Exception Handling: Exceptions, handling exceptions using try-catch, catching multiple exceptions, using the finally clause, types of exceptions, throwing user-defined exceptions.

UNIT-IV

Multithreading: Introduction to multithreading, the main thread, Java thread model, thread priorities, synchronization in Java, and inter-thread communication.

I/O in Java: I/O basics, streams and stream classes, predefined streams, reading from and writing to the console, reading and writing files, the transient and volatile modifiers, and using native methods.

Strings and Characters: Fundamentals of characters and strings, the String class, string operations, data conversion using valueOf() method, the StringBuffer class, and its methods.

BOOKS:

1. Tenenbaum, A. S. Modern Operating Systems. Prentice Hall.
2. Godbole, A. Operating Systems. Tata McGraw-Hill.
3. Peterson, J. L., & Silberschatz, A. Operating System Concepts. Addison-Wesley Publishing Company.
4. Deitel, H. M. An Introduction to Operating Systems. Addison-Wesley Publishing Company.
5. Kernighan, B., & Pike, R. The UNIX Programming Environment. Prentice Hall.

6. Bach, M. J. Design of the UNIX Operating System. Prentice Hall.
7. Prato, S. Advanced UNIX: Programmer's Guide. BPB Publications.
8. Das, S. UNIX Concepts and Applications: Featuring SCO UNIX and LINUX. Tata McGraw-Hill.

PROGRAMMING IN JAVA LAB

Note: At least 8 experiments are to be performed by the students.

List of Subject related Experiments:

1 a) Write a java program to find the Fibonacci series using recursive and non-recursive functions

b) Write a java program to multiply two given matrices.

c) Write a java program for Method overloading and Constructor overloading

2 a) Write a program to demonstrate execution of static blocks, static variables & static methods.

b) Write a program to display the employee details using Scanner class

c) Write a program for sorting a given list of names in ascending order

3 a) Write a program to implement single and Multi-level inheritance

b) Write a program to implement Hierarchical Inheritance.

c) Write a program to implement method overriding.

4 a) Write a program to create an abstract class named Shape that contains two integers and an empty method named printArea (). Provide three classes named Rectangle, Triangle and Circle such that each one of the classes extends the class Shape. Each one of the classes contains only the method printArea () that prints the area of the given shape.

b) Write a program to implement Interface.

c) Write a program to implement multiple and Hybrid Inheritance

5 a) Write a program to create inner classes

b) Write a program to create user defined package and demonstrate various access modifiers.

c) Write a program to demonstrate the use of super and final keywords.

6 a) Write a program if number is less than 10 and greater than 50 it generate the exception out of range. else it displays the square of number.

b) Write a program with multiple catch Statements.

c) Write a program to implement nested try

7 a) Write a Program to implement simple Thread by extending Thread class and implementing runnable interface.

b) Write a program that implements a multi-thread application that has three threads

c) Write a program to set and print thread priorities.

241/CS/CC203

ANALYSIS AND DESIGN OF ALGORITHMS

Semester	2			
Course code	CC-A06			
Category	Core Course(s)			
Course title	Analysis and Design of Algorithms			
Course ID	241/CS/CC203			
Scheme and Credits	L	T	P	Credits
	3	0	1	4
Theory Internal	25 marks			
Theory External	50 marks			
Practical Internal	5 marks			
Practical External	20 marks			
Total	100 marks			
Duration of Exam	3 hrs			

Note:*The examiner will set nine questions in total. Question one will have seven parts from all units and the marks of first question will be of 20% of total marks of Question Paper and the remaining eight questions to be set by taking two questions from each unit and the marks of each question from Question no.2 to 9 will be of 20% of total marks of Question paper. The students have to attempt five questions in total, the first being compulsory and selecting one from each unit.*

COURSEOUTCOMES:

At the end of this course, students will demonstrate the ability to

CO1: Able to Argue the correctness of algorithms using inductive proofs and analyze worst-case running times of algorithms using asymptotic analysis.

CO2: Able to explain important algorithmic design paradigms (divide-and-conquer, greedy method, dynamic-programming and Backtracking) and apply when an algorithmic design situation calls for it.

CO3: Able to Explain the major graph algorithms and Employ graphs to model engineering problems, when appropriate.

CO4: Able to Compare between different data structures and pick an appropriate data structure for a design situation

CO5: Able to Describe the classes P, NP, and NPComplete and be able to prove that a certain problem is NP-Complete.

CO6: Able to analyze String matching algorithms.

UNIT - I

Introduction to Algorithms: Algorithm, Performance Analysis (Time and Space complexity), Asymptotic Notation (Big O, Omega and Theta)-best, average and worst-case behaviour.Elementary Data Structures (Basic terminology of Stacks and Queues, Tree, Graph), Sets andDisjoint Set Union.

Divide and Conquer: General method, Binary Search, Merge Sort, Quick Sort, and other sorting algorithms with divide and conquer strategy, Strassen's Matrix Multiplication algorithms and analysis of these problems.

UNIT - II

Greedy Method: General method, Fractional Knapsack problem, Job Sequencing with Deadlines, Minimum Cost Spanning Trees, Single source shortest paths.

Dynamic Programming: General method, Optimal Binary Search Trees, 0/1 knapsack, The Traveling Salesperson problem.

UNIT - III

Back Tracking: General method, The 8-Queen's problem, Sum of subsets, Graph Colouring, Hamiltonian Cycles.

Branch and Bound: The method, 0/1 knapsack problem, Traveling Salesperson problem, Efficiency considerations.

UNIT - IV

NP Hard and NP Complete Problems: Basic concepts, Cook's theorem, NP hard graph problems, NP hard scheduling problems, NP hard code generation problems, and Some simplified NP hard problems.

TEXT AND REFERENCE BOOKS:

1. Fundamental of Computer algorithms, Ellis Horowitz and Sartaj Sahni, 1978, Galgotia Publication

2. Introduction to Algorithms, Thomas H Cormen, Charles E Leiserson and Ronald L Rivest: 1990,TMH

3. The Design and Analysis of Computer Algorithm, Aho A.V. Hopcroft J.E., 1974, AddisonWesley.

4. Algorithms-The Construction, Proof and Analysis of Programs, Berlion, P.Bizard, P.,

1986Johan Wiley & Sons,

5. Writing Efficient Programs, Bentley, J.L., PHI

6. Introduction to Design and Analysis of Algorithm, Goodman, S.E. &Hedetnieni, 1997, MGH.

7. Introduction to Computers Science- An algorithms approach, Jean Paul Trembley, RichardB.Bunt, 2002, T.M.H.

8. Fundamentals of Algorithms: The Art of Computer Programming Vol Knuth, D.E.: 1985, Naresh Publication.

ANALYSIS AND DESIGN OF ALGORITHMS LAB

List of Subject related Experiments:

1. Write a program to implement different sorting techniques. • Bubble Sort • Insertion Sort • Selection Sort • Quick Sort • Merge Sort
2. Write a program to find minimum cost spanning tress.
3. Write a program to implement travelling sales person problem.
4. Write a program to find Longest Path in a Directed Acyclic Graph.
5. Write a program for Shortest path with exactly k edges in a directed and weighted graph.
6. Write a program find maximum number of edge disjoint paths between two vertices
7. Implement 0/1 Knapsack problem using Dynamic Programming.
8. Perform various tree traversal algorithms for a given tree.
9. Implement N-Queens Problem

241|CS|DS201

DISCRETE MATHEMATICS & STATISTICS

Semester	2			
Course code	DSE-02			
Category	Discipline Specific Elective Courses			
Course title	Discrete Mathematics & Statistics			
Course ID	241|CS|DS201			
Scheme and Credits	L	T	P	Credits
	2	1	0	3
Theory Internal	25 marks			
Theory External	50 marks			
Total	75 marks			
Duration of Exam	3 hrs			

Note: *The examiner will set nine questions in total. Question one will have seven parts from all units and the marks of first question will be of 20% of total marks of Question Paper and the remaining eight questions to be set by taking two questions from each unit and the marks of each question from Question no.2 to 9 will be of 20% of total marks of Question paper. The students have to attempt five questions in total, the first being compulsory and selecting one from each unit.*

COURSEOUTCOMES:

At the end of this course, students will demonstrate the ability to

CO1: To solve mathematical problems based on concepts of set theory, relations, functions and lattices.

CO2: To express logical sentences in terms of quantifiers and logical connectives.

CO3: To apply basic counting techniques to solve permutation and combination problems.

CO4: To solve recurrence relations.

CO5: To classify the algebraic structure of any given mathematical problem.

CO6: To evaluate Boolean functions and simplify expressions using the properties of Boolean algebra.

UNIT-I

SET THEORY, RELATIONS, FUNCTIONS, LOGIC AND PROPOSITIONAL CALCULUS

Set Theory: Introduction to set theory, Venn diagrams, Set operations, Algebra of sets, Duality, Finite and infinite sets, Counting principles, Power sets, Partitions, and Multi sets.

Relations: Cartesian product, Representation of relations, Types of relation, Binary relation, Equivalence relations, Partitions, Partial ordering relations, POSET, Hasse diagram, Lattices and its types.

Functions: Definition, Types of functions, Bijective functions, Composition of functions, Inverse functions, recursively defined functions, Finite and infinite sets, Countable and uncountable sets, Cantor's diagonal argument and The Power Set theorem, Schroeder-Bernstein theorem.

Logic And Propositional Calculus: Introduction, Propositions and compound propositions, Logical operations, Propositions and truth tables, Tautologies, Contradictions, Logical equivalence, Algebra of propositions, Conditional and Bi-conditional statements, The use of Quantifiers.

UNIT-II

Basic Counting Techniques: Pigeon-hole principle, Permutation and Combination, the Division algorithm: Prime Numbers, The GCD: Euclidean Algorithm, The Fundamental Theorem of Arithmetic.

Recursion And Recurrence Relation: Polynomials and their evaluation, Sequences, Introduction to AP, GP and AG Series, Partial Fractions, Recurrence Relation, Linear Recurrence Relations with Constant Coefficients, Linear Homogeneous Recurrence Relations with Constant Coefficients, Particular Solution- Homogeneous Linear Difference Equations, Non-Homogeneous Linear Difference Equations, Total Solution, solving recurrence relation using generating functions.

UNIT-III

Definitions and examples of Algebraic Structures with one Binary Operation: Semi Groups, Monoids, Groups, Semigroups, Subgroups, Abelian groups, Cosets, Normal Subgroup, Cyclic groups, Congruence Relation and Quotient Structures, Permutation Groups, Lagrange's Theorem, Homomorphism, Isomorphism, Automorphism.

Definitions and examples of Algebraic Structures with two Binary Operation: Rings, Integral Domain, Fields; Boolean Algebra and Boolean Ring, Identities of Boolean Algebra, Duality, Representation of Boolean Function, Disjunctive and Conjunctive Normal Form.

UNIT-IV

GRAPHS THEORY: Introduction to graphs and their properties, Degree, Connectivity, Path, Cycle, Directed and undirected graphs, Subgraph, Bipartite Graphs, Regular Graphs,

Connected Graphs, Multigraph and Weighted graph, Homomorphic and Isomorphic graphs, cut points and bridges, Paths and circuits, shortest path algorithm for weighted graphs, Eulerian paths and circuits, Hamiltonian path and circuits, Planar Graphs, Euler's formulae, Graph Colouring.

BOOKS:

1. Kenneth H. Rosen, *Discrete Mathematics and its Applications*, 6th Edition, Tata McGraw Hill, 2011.
2. Satinder Bal Gupta: *A Text Book of Discrete Mathematics and Structures*, University Science Press, Delhi.
3. C. L. Liu and D. P. Mohapatra, *Elements of Discrete Mathematics A Computer Oriented Approach*, Tata McGraw Hill, 3rd Edition, 2008.
4. J.P. Trembley and R. Manohar, *Discrete Mathematical Structures with Applications to Computer Science*, Tata McGraw Hill – 13th reprint, 2012.
5. Richard Johnsonbaugh, *Discrete Mathematics*, 6th Edition, Pearson Education Asia, 2011.
6. S. Lipschutz and M. Lipson, *Discrete Mathematics*, Tata McGraw Hill, 3rd Edition, 2010.
7. B. Kolman, R. C. Busby and S. C. Ross, *Discrete Mathematical structures*, 6th Edition, PHI,2010.

241/CS/DS202

MOBILE COMPUTING

Semester	2			
Course code	DSE-02			
Category	Discipline Specific Elective Courses			
Course title	Mobile Computing			
Course ID	241/CS/DS202			
Scheme and Credits	L	T	P	Credits
	2	1	0	3
Theory Internal	25 marks			
Theory External	50 marks			
Total	75 marks			
DurationofExam	3 hrs			

Note: *The examiner will set nine questions in total. Question one will have seven parts from all units and the marks of first question will be of 20% of total marks of Question Paper and the remaining eight questions to be set by taking two questions from each unit and the marks of each question from Question no.2 to 9 will be of 20% of total marks of Question paper. The students have to attempt five questions in total, the first being compulsory and selecting one from each unit.*

COURSE OUTCOMES:

At the end of this course, students will demonstrate the ability to

CO1: Gain the knowledge about various types of Wireless Data Networks and Wireless Voice Networks

CO2: Understand the architectures, the challenges and the Solutions of Wireless Communication.

CO3: Realize the role of Wireless Protocols in shaping the future Internet.

CO4: Able to develop simple Mobile Applications Using Toll kit.

UNIT - I

Mobile Physical Layer: Review of generation of mobile services, overview of wireless telephony, cellular concept, GSM: air-interface, channel structure, location management: HLR-VLR, hierarchical, handoffs, channel allocation in cellular systems, CDMA, GPRS.

Mobile Computing Architecture: Issues in mobile computing, three tier architecture for mobile computing, design considerations, Mobile file systems, Mobile databases. WAP: Architecture, protocol stack, Data gram protocol, Wireless transport layer security, Wireless transaction protocol, wireless session protocol, application environment, and applications.

UNIT - II

Mobile Data Link Layer: Wireless LAN over view, IEEE 802.11, Motivation for a specialized MAC, Near & far terminals, Multiple access techniques for wireless LANs such as collision avoidance, polling, Inhibit sense, spread spectrum, CDMA, LAN system architecture, protocol architecture, physical layer MAC layer and management, Hiper LAN.

Blue Tooth: IEEE 802.15 Blue tooth User scenarios, physical, MAC layer and link management. Local Area Wireless systems: WPABX, IrDA, ZigBee, RFID, WiMax.

UNIT - III

MOBILE IP Network Layer: IP and Mobile IP Network Layer- Packet delivery and Handover Management- Location Management- Registration- Tunnelling and Encapsulation- Route Optimization- Dynamic Host Configuration Protocol, Ad Hoc networks, localization, MAC issues, Routing protocols, global state routing (GSR), Destination sequenced distance vector routing (DSDV), Dynamic source routing (DSR), Ad Hoc on demand distance vector routing (AODV), VoIP –IPSec.

Mobile Transport Layer: Traditional TCP/IP, Transport Layer Protocols-Indirect, Snooping, Mobile TCP.

UNIT - IV

Support for Mobility: Data bases, data hoarding, Data dissemination, UA Prof and Caching, Service discovery, Data management issues, data replication for mobile computers, adaptive clustering for mobile wireless networks, Mobile devices and File systems, Data Synchronization, Sync ML.

Introduction to Wireless Devices and Operating systems: Palm OS, Windows CE, Symbion OS, Android, Mobile Agents. Introduction to Mobile application languages and tool kits.

BOOKS:

1. J. Schiller, —Mobile Communicationsl, 2nd edition, Pearson, 2011.
2. Raj Kamal —Mobile Computingl Oxford Higher Education, Second Edition, 2012.
3. Dharam prakash Agrawal and Qing-An Zeng, —Introduction to Wireless and Mobile Systemsl 3rd edition,Cengage learning 2013.
4. Asoke K Talukder, Hasan Ahmed,Roopa R Yavagal —Mobile Computingl, Tata McGraw HillPub ,Aug – 2010
5. Pei Zheng, Larry L. Peterson, Bruce S. Davie, Adrian Farrell —Wireless Networking Completel MorganKaufmann Series in Networking , 2009 (introduction, WLAN MAC)
6. Vijay K Garg —Wireless Communications & Networkingl Morgan Kaufmann Series, 2010

7. M. V. D. Heijden, M. Taylor, Understanding WAP, Artech House.
8. Charles Perkins, Mobile IP, Addison Wesley.
9. Charles Perkins, Ad hoc Networks, Addison Wesley.
10. Uwe Hansmann, Lothar Merk, Martin S. Nicklous, Thomas Stober, —Principles of Mobile Computing,Springer.
11. Evaggelia Pitoura and George Samarus, —Data Management for Mobile Computingl, Kluwer Academic Press, 1998