**Department of Computer Science & Informatics**

**University of Kota, Kota**

M.B.S. Marg, Near Kabir Circle, KOTA - 324005

Website: [www.uok.ac.in](http://www.uok.ac.in)

**MCA – III Semester**

**Tentative Lecture Plan of Paper - 1**

**MCA 301 – Information and Network Security System**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Unit** | **Topic** | **Lecture No.** |
| 1. | I | Basic Security Concept, Computer Security | 1-2 |
| 2. | Threats to Security, | 3 |
| 3. | attacks | 4-5 |
| 4. | Security services & Mechanisms, Communication | 6 |
| 5. | Security-Encryption, Classical Encryption Model | 7 |
| 6. | Steganography. | 8 |
| 7. | II | Cryptography- transposition/ substitution, Caesar Cipher  | 9-10 |
| 8. | Cryptosystem, Symmetric and Asymmetric crypto primitives | 11 |
| 9. | Private Key Cryptography, Block Cipher Principles | 12-13 |
| 10. | Data encryption Standards, Encryption and Decryption using round functions, | 14-15 |
| 11. | AES, Triple DES, Random number generation, Key distribution.  | 16-17 |
| 12. | III | Message Authentication and hash functions  | 18 |
| 13. | message digest, strong and weak collision, message authentication code, | 19-21 |
| 14. | MD5, Hash functions, Secure Hash algorithm (SHA) | 22-23 |
| 15. | Birthday paradox | 24 |
| 16. | digital signature, Digital signature standards (DSS). | 25 |
| 17. | IV | Public Key Cryptography – Number Theory: Euclidean algorithm, Euler Theorem, ,  | 26-27 |
| 18. | Fermat theorem, Totent function, multiplicative and additive inverse. | 28-29 |
| 19. | Principles of Public key cryptography, Public Key infrastructure (PKI), | 30 |
| 20. | RSA algorithm | 31-32 |
| 21. | Key management | 33 |
| 22. | Elliptic Curve cryptography, | 34 |
| 23. | Diffie Hellman Key Exchange.  | 35 |
| 24. | V | Network and System Security – Network Attacks | 36 |
| 25. | IP Security (IPSec): AH & ESP | 37-38 |
| 26. | Web security: SSL /TLS, Kerberos | 39 |
| 27. | E-mail Security: Pretty good Privacy (PGP), S/Mime | 40-41 |
| 28. | Network scanning, System security: intruders, viruses, firewall Design Principles | 42-43 |
| 29. | Intrusion Detection system ( IDS), | 44 |
| 30. | Concept of Cyber Security. | 45 |

 **(Changes in contents, if any will be notified)**

**Text/Reference Books**

1. Cryptography and Network Security by Willian Stallings, Pearson Education, 6th edition, 2013.
2. Cryptography and Network Security by Behrouz A. Forouzen, Tata McGraw Hill.
3. Cryptography and Network Security by atul Kahate, McGraw Hill Education India (Pvt. Ltd.) 2nd edition, 2009.
4. Handbook of Information Security Management, Micki Krause F tipton- Vol. – 3, CRC Press LLC, 2004.
5. Link: Dr, Gary C. Kersler’s An overview of Cryptography: “Pretty good Privacy (PGP)”(HTML).
6. www.Netseurity.net.

**Department of Computer Science & Informatics**

**University of Kota, Kota**

M.B.S. Marg, Near Kabir Circle, KOTA - 324005

Website: [www.uok.ac.in](http://www.uok.ac.in)

**MCA – III Semester**

**Tentative Lecture Plan of Paper - 1**

**MCA 302 – Programming with JAVA**

**(Changes in contents, if any will be notified)**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Unit** | **Topic** | **Lecture No.** |
| 1. | I | An overview of Java, JVM, byte code | 1 |
| 2. | I | Java class libraries | 2 |
| 3. | I | Data types | 3 |
| 4. | I | Variable | 4 |
| 5. | I | Data types and casting, Operators | 5-6 |
| 6. | I | operator precedence and Control statements | 7-8 |
| 7. | II | Declaring object reference variable | 9-10 |
| 8. | II | Introducing methods | 11 |
| 9. | II | constructors, the key word | 12 |
| 10. | II |  garbage collection | 13-14 |
| 11. | II | Overloading methods | 15-16 |
| 12. | II | String handling,. | 17 |
| 13. | II | String buffer | 18 |
| 14. | III | Inheritance and polymorphism | 19 |
| 15. | III | super class and subclass, | 20 |
| 16. | III | protected members, Relationship between super and sub class | 21-22 |
| 17. | III | Inheritance hierarchy, | 23 |
| 18. | III | abstract classes and methods | 24 |
| 19. | III | final methods and classes | 25 |
| 20. | III | nested classes, | 26 |
| 21. | III | Packages and Interfaces,  | 27 |
| 22. | III | Defining a package, importing package, | 28 |
| 23. | III | defining an interface, implementing and applying interfaces. | 29-30 |
| 24. | IV | Exception Handling Fundamentals | 31-32 |
| 25. | IV |  exception types | 33 |
| 26. | IV | using try and catch | 34 |
| 27. | IV | File handling | 35-36 |
| 28. | IV | Character based file and binary file, | 37 |
| 29. | IV | Multithreaded Programming: | 38 |
| 30. | IV | Creating a single and multiple threads | 39 |
| 31. | IV | thread priorities, synchronization. | 40 |
| 32. | V | Applets: Applets basics, applets architecture | 41 |
| 33. | V | applets skeleton, the html applet tag | 42 |
| 34. | V | passing parameters in applets, event-handling:  | 43 |
| 35. | V | event classes and event listener interfaces | 44 |
| 36. | V | introduction to swing and servelets. | 45 |

**Text/Reference Books:**

1. The complete reference Java - 2, P. Naughton and H. Schildt: Tata Mc-Graw Hill.

2. the java hand books, Patrick Naughton, Michael Morrison, Osborne/McGraw-Hill

3. A Desktop Quick Reference for Java Programmers, David Flanagan, Java in a Nutshell: O'Reilly & Associates, Inc.

4. Programming with Java A Primer, E. Balaguruswamy, TMH.

5. Big Java, Cay Horstmann, Wiley India edition, 2nd Edition.

6. Core Java, Dietel and Dietel, Pearson/Pretice Hall , 7th Edition.

7. Internet and Web-Technologies by Rajkamal, TataMcGraw-Hill, 6th Edition, 2011.

**Department of Computer Science & Informatics**

**University of Kota, Kota**

M.B.S. Marg, Near Kabir Circle, KOTA - 324005

Website: [www.uok.ac.in](http://www.uok.ac.in)

**MCA – III Semester**

**Tentative Lecture Plan of Paper - 3**

**MCA 303 – Theory of Computation**

**(Changes in contents, if any will be notified)**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Unit** | **Topic** | **Lecture No.** |
| 1. | I | Mathematical preliminaries,  | 1 |
| 2. | I | alphabets, strings, Languages, states, transitions, | 2-3 |
| 3. | I | finite automata  | 4-6 |
| 4. | I | regular expressions, applications e.g. Lexical analyzers and text editors | 7-9 |
| 5. | II | The pumping Lemma  | 10-12 |
| 6. | II | closure property of regular sets | 13-15 |
| 7. | II | Decision algorithms for regular sets. | 16-18 |
| 8. | III | Context free grammars, | 19-21 |
| 9. | III | Chomsky and Greibach normal form theorems,  | 22-24 |
| 10. | III | ambiguity, Pushdown automata  | 25-27 |
| 11. | III | equivalence of context free languages to sets accepted by non-deterministic PDA,  | 28-29 |
| 12. | III | the Pumping Lemma for CFL’s,  | 30 |
| 13. | III | closure properties of CFL’s and decision algorithms for CFL’s | 31-32 |
| 14. | IV | Turing Machines: Introduction, Turing hypothesis,  | 33 |
| 15. | IV | Turing computability, nondeterministic, multitape and other versions of Turing machine,  | 34 |
| 16. | IV | Church’s hypothesis, primitive recursive function, | 35 |
| 17. | IV | Generalization, recursively enumerable Languages and Turing Computability | 36-37 |
| 18. | V | Undesirability: Universal Turing machines and unsolvability of the  | 38-39 |
| 19. | V | halting problem. | 40 |
| 20. | V | an undecidable problem,  | 41 |
| 21. | V | Post’s Correspondence problem. | 42-43 |
|  |  | Problem solving | 44-45 |

**Text/Reference Books**

1. Introduction to Automata Theory, Languages and Computation,Hopcroft J.E. and Ullman J.D., Narosa Publishing House, 1988.

2. Theory of Computation, Derickwood, Harper & Row Publishers, New York, 1987.

3. Elements of the Theory of Computation,Lewis H.R. & Papadimitriou C.H, Prentice Hall International Inc. 1981.

 4. Introduction to the Theory of Computation, Michal Sipear, MA.: Thomson course technology, 2nd edition, 2006.

5. Automata Theory, language and Computation, J. Hoperoft, R. Motwani and Jeffery Ullman, Addison wisely, 3rd edition, 2013.

6. Theory of Computer Science: Automata, Language and computation, K.L.P. Mishra, N. Chandrasekaran, PHI Learning Pvt. Ltd.

**Department of Computer Science & Informatics**

**University of Kota, Kota**

M.B.S. Marg, Near Kabir Circle, KOTA - 324005

Website: [www.uok.ac.in](http://www.uok.ac.in)

**MCA – III Semester**

**Tentative Lecture Plan of Paper - 1**

**MCA 304 – Design and Analysis of Algorithms**

**(Changes in contents, if any will be notified)**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **Unit** | **Topics to be Covered** | **Lecture No.** |
| 1 | I | Algorithms and structured programming | 1-2 |
| 2 | I | analysing algorithms | 3-4 |
| 3 | I | behaviour of an algorithm | 5-6 |
| 4 | I | Order notations | 7-8 |
| 5 | I | Time and space complexities (polynomial, logrithmic and exponential), | 9-10 |
| 6 | I | average and worst case analysis | 11 |
| 7 | I | lower and upper bounds | 12 |
| 8 | II | Advanced data structures (Intro) | 13 |
| 9 | II | Threaded trees, B-trees | 14-15 |
| 10 | II | Heaps and heapsort | 16-17 |
| 11 | II | sets and relations | 18 |
| 12 | II | Graphs | 19-20 |
| 13 | II | Hashing | 21 |
| 14 | II | Basic search & Traversal Techniques (Breadth first traversals of Graphs) | 22-23 |
| 15 | II | and Depth first traversals of Graphs | 24 |
| 16 | III | Algorithm design strategies: Divide and conquer | 25-26 |
| 17 | III | Mergesort,  | 27 |
| 18 | III | Quicksort, | 28 |
| 19 | III | matrix multiplication | 29 |
| 20 | III | Greedy method: General method | 30 |
| 21 | III | knapsack problem,  | 31-32 |
| 22 | III |  job sequencing with deadlines | 33 |
| 23 | III | minimum cost spanning trees. | 34 |
| 24 | III | Dynamic programming (0/1 knapsack, travelling salesman problem) | 35 |
| 25 | IV | Backtracking (8 - Queens problem, Sum of Subsets, Graph coloring, 0/1 Knapsack).  | 36-38 |
| 26 | IV | Branch & Bound (0/1 knapsack, Travelling salesman). | 39-40 |
| 27 | V | Approximation algorithms: Polynomial Time Approximation Schemes. - Cook's theorem, NP completeness reductions.  | 41-42 |
| 28 | V | Complexity: - NP-Hard and NP-complete Problems | 43-44 |
| 29 | V | Cook's theorem, NP completeness reductions.  | 45-46 |

**Text/Reference Books:**

1. E. Horowitz, S. Sahani, Fundamentals of Computer Algorithms, Galgotia Publications, 1985.

2. Aho, J.E. Hopcroft, & J.D. Ullman, Design & Analysis of Computer Algorithms, Addition Wesley, 1974.

3. P.Berlions & P. Bizard, Algorithms - The Construction, Proof & Analysis of Programs, John Wiley & Sons, 1986.

4. K. Melhorn, Data Strucures and Algorithms, Vol. I & II, Springer Verlag, 1984.