

Centre for Computer Science & Technology

Proposed

Course Structure and Syllabus

For

**M.Tech in Computer Science & Technology
(Cyber Security)**

Eligibility Criteria: B.Tech. / B.E. in Computer Science and Engineering / Information Technology / Electronics / Electronics & Communication from a recognized Indian or foreign university with minimum 55% marks. Preference will be given to candidates having valid GATE score.

Centre for Computer Science & Technology
Scheme of Programme: M.Tech. in Computer Science & Technology (Cyber Security)

SEMESTER 1

S.No	Paper Code	Course Title	L	T	P	Cr	% Weightage				E
							A	B	C	D	
1	CBS.501	Research Methodology and Statistics	4	-	-	4	25	25	25	25	100
2	CBS.502	Advanced Data Structures and Algorithms	4	-	-	4	25	25	25	25	100
3	CBS.503	Advanced Computer Networks	4	-	-	4	25	25	25	25	100
4	CBS.504	Operating System Internals	4	-	-	4	25	25	25	25	100
5	CBS.505	Advanced Data Structures and Algorithms - Lab	-	-	4	2	-	-	-	-	50
6	CBS.506	Advanced Computer Networks - Lab	-	-	4	2	-	-	-	-	50
7	CBS.507	Seminar 1	-	-	4	2	-	-	-	-	50
8		Inter-Disciplinary Elective -1 (From Other Departments)	2	-	-	2	10	15	15	10	50
			18	-	12	24					600

A: Continuous Assessment: Based on Objective Type Tests

B: Pre-Scheduled Test-1: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

C: Pre-Scheduled Test-2: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

D: End-Term Exam (Final): Based on Objective Type Tests

E: Total Marks

L: Lectures T: Tutorial P: Practical Cr: Credits

SEMESTER 2

S.No	Paper Code	Course Title	L	T	P	Cr	% Weightage				E
							A	B	C	D	
1	CBS.508	Information Security	4	-	-	4	25	25	25	25	100
2	CBS.509	Python Programming	4	-	-	4	25	25	25	25	100
3	CBS.510	Computer and Cyber Forensics	4	-	-	4	25	25	25	25	100
4	Opt any one course from following three courses										
	CBS.511	Emerging Technologies	4	-	-	4	25	25	25	25	100
	CBS.512	Wireless LAN and Mobile Computing									
	CBS.513	Advanced Database Management Systems									
5	CBS.514	Information Security - Lab	-	-	4	2	-	-	-	-	50
6	CBS.515	Python Programming - Lab	-	-	4	2	-	-	-	-	50
7	CBS.516	Research Seminar	-	-	4	2	-	-	-	-	50
8		Inter-Disciplinary Elective-2 (From Other Departments)	2	-	-	2	10	15	15	10	50
			18	-	12	24					600

A: Continuous Assessment: Based on Objective Type Tests

B: Pre-Scheduled Test-1: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

C: Pre-Scheduled Test-2: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

D: End-Term Exam (Final): Based on Objective Type Tests

E: Total Marks

L: Lectures T: Tutorial P: Practical Cr: Credits

SEMESTER 3

S.No	Paper Code	Course Title	L	T	P	Cr	% Weightage				E
							A	B	C	D	
1	CBS.601	Network Security	4	-	-	4	25	25	25	25	100
2	CBS.602	Cyber Laws	4	-	-	4	25	25	25	25	100
3	CBS.603	Network Security- Lab	-	-	4	2	-	-	-	-	50
4	CBS.604	Seminar 2	-	-	4	2	-	-	-	-	50
5	CBS.605	Dissertation Part-1	-	-	-	12					300
			08	-	8	24					600

SEMESTER 4

S.No	Paper Code	Course Title	L	T	P	Cr	% Weightage				E
							A	B	C	D	
1	CBS.606	Ethical Hacking	4	-	-	4	25	25	25	25	100
2	CBS.607	Ethical Hacking Lab	-	-	4	2	-	-	-	-	50
3	CBS.608	Seminar 3	-	-	4	2	-	-	-	-	50
4	CBS.609	Dissertation Part-2	-	-	-	16					400
			04	-	08	24					600

A: Continuous Assessment: Based on Objective Type Tests

B: Pre-Scheduled Test-1: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

C: Pre-Scheduled Test-2: Based on Objective Type & Subjective Type Test (By Enlarged Subjective Type)

D: End-Term Exam (Final): Based on Objective Type Tests

E: Total Marks

L: Lectures T: Tutorial P: Practical Cr: Credits

SEMESTER 1

CBS.501

Research Methodology and Statistics

Credit Hours: 4

Objective: The objective of this course is to ensure that a student learns basis of scientific research and statistical methods to arrive at and verify the conclusions drawn.

Unit 1

14 Hours

General principles of research: Meaning and importance of research, Critical thinking, Formulating hypothesis and development of research plan, Review of literature, Interpretation of results and discussion.

Technical writing: Scientific writing, Writing synopsis, Research paper, Poster preparation and Presentations and Dissertation.

Unit 2

14 Hours

General Statistics: Difference between parametric and non-parametric statistics, Univariate and multivariate analysis, Confidence interval, Errors, Levels of significance, Hypothesis testing, Measures of central tendency and dispersal, Histograms, Probability distributions (Binomial, Poisson and Normal), Sampling distribution, Kurtosis and skewness..

Unit 3

14 Hours

Comparative Statistics: Comparing means of two or more groups: Student's t-test, Paired t-test, One-way and two-way analysis of variance (ANOVA), Critical difference (CD), Fisher's LSD (Least significant difference), Kruskal-Wallis one-way ANOVA by ranks, Friedman two-way ANOVA by ranks, Chi-square test.

Unit 4

14 Hours

Regression and correlation: Standard errors of regression coefficients, Comparing two regression lines, Pearson Product – Moment Correlation Coefficient, Spearman Rank correlation coefficient, Power and sampling size in correlation and regression.

Text books:

1. Kothari, C.R. (2008). Research Methodology: Methods and Techniques. 2nd ed. New Age International.
2. Gall, J.P., Borg, W.R. and Gall, M.D. (2006). Educational Research: An Introduction. Prentice Hall.
3. Norman, G. and Streiner, D. (2008). Biostatistics: The Bare Essentials. 3/e (with SPSS). Decker Inc. USA

Suggested readings:

1. William, W. (2009). Research Methods in Education. India: Pearson Education.
2. Best J. W. (1999). Research in Education, New Delhi: Prentice Hall of India Pvt. Ltd.

Objective: This course will emphasize on advance data structures and algorithm analysis. Various problem solving techniques will be explained as a part of the course. This course will also help in detailed understanding of data structures e.g. Red-Black Trees and Splay Trees. Pattern matching algorithms will also be taught. Pre-requisite for this course is data structure

Unit 1**14 Hours**

Introduction to algorithm concepts: Algorithm analysis, Order Notation, Recurrence relations. Design strategies: Divide-and-conquer: Binary Search, Bubble Sort, Merge Sort, Quick Sort, Randomized Quick Sort, Insertion Sort, Greedy Method: Activity Selection & Knapsack Problem.

Unit 2**14 Hours**

Dynamic Programming: Matrix Chain Multiplication problem, Backtracking: 8 Queen's problem
Data structures: Stack, Queue, Priority Queue, Hash table, Heaps, Heap Sort.
Search trees: Binary search trees, AVL trees, Red-Black, Splay Trees, M-way trees: B-Trees.

Unit 3**14 Hours**

Pattern matching and Tries: Pattern matching algorithms-Brute force, the Boyer -Moore algorithm, the Knuth-Morris-Pratt algorithm, Standard Tries, Compressed Tries, Suffix tries.
Advanced data structure: Fibonacci Heaps, Data structures for disjoint sets.

Unit 4**14 Hours**

Graph algorithms: Basics of Graph structures, Elementary graph algorithms, Minimum Spanning trees: Prim's algorithm and Kuruskal's algorithm, Single-Source and All Pairs Shortest Path algorithms, Max flow problem and its solutions.

Text books:

1. Cormen, T.H., Leiserson, C.E., Rivest, R.L. and Stein, C. 2009. Introduction to Algorithms. 3rd ed. Mit Press.
2. Lipschutz, S. 2009. Data Structures with C. Tata McGraw-Hill Education.
3. Sahni S., Data structures, Algorithms and Applications in C++, 2nd edition, Press Orient Longman Pvt. Ltd.

Suggested readings:

1. Aho, A.V., Hopcroft, J.E. and Ullman, J. D. 2009. Data Structures and Algorithms. India: Pearson Education.
2. Weiss, M.A. 2009. Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson Education.
3. Drozdek, A., Data structures and algorithms in C++, 3rd Edition, Thomson

Objective: The course is structured to uncover and understand the current directions of computer networks from literature readings and to encourage a performance perspective towards analysis of computer and communications networks. Topics are covered in some depth, including both abstract and concrete aspects. The Emphasis of course is on various advanced internetworking and routing techniques. It helps to “fill-in” gaps in students’ networking knowledge.

Unit 1**14 Hours**

Introduction: Evolution of Computer Networks, Concept of Layering, Network: Categories, Components, Connections; Applications of Computer Networks, Network Standardization, Network Characteristics, Data Communication: Signaling, Modulation, Multiplexing, Transmission and Errors; Transmission Media: Cable types, Wireless Transmission.

Unit 2**14 Hours**

Local and personal Area Networks: IEEE802.3 Ethernet, IEEE 802.11 and WLANs, IEEE 802.16 (WiMax), IEEE 802.15 Wireless Personal Area Networks: IEEE 802.15.3-A Ultra Wideband Wireless Personal Area Networks, IEEE 802.15.4 ZigBee.

Wide Area Networks: Internet: Infrastructure, Addressing, Bridges, Switches, Routers; Cellular Networks: Architecture, Mechanisms to support a Mobile Environment, Protocol Stack in Cellular networks, Deployment.

Unit 3**14 Hours**

Internetworking: Concepts, Architecture and Protocols, IP-Internet Protocol Addresses, Binding Protocol Addresses, IP-Datagram, IP-Encapsulation, Fragmentation and Re-assembly, Future IP (IPv6), Error Reporting Mechanism (ICMP), Datagram Transport Service (UDP), Reliable Transport Service (TCP), Internet Routing.

Unit 4**14 Hours**

Mobile Ad-hoc Networks: Routing Protocols, Modeling and Simulation Tools, Communication Protocols of MANETs, Future Networks: Vehicular Ad-hoc Networks, Wireless Sensor Networks, Under Water Wireless Ad-hoc Networks, Under Water Sensor Networks, Wireless Mesh Networks.

Text books:

1. Trivedi, B. 2013. Computer Networks. Oxford University Press.
2. Kurose, J. F. and Ross, K. W. 2010. Computer Networking – A top-down approach featuring the Internet, 3rd Ed. India: Pearson Education.
3. Olifer, N. and Olifer, V. 2012. Computer Networks: Principles, Technologies and Protocols for Network Design. India: John Wiley & Sons.
4. Forouzan, B.A., 2009, Data Communications and Networking, 4th Ed. Tata McGraw Hill Education.

Suggested readings:

1. Peterson L. L. and Davie B. S. 2011. Computer Networks: A System Approach, 5th Ed. India: Elsevier.
2. Comer, D. E. and Narayanan, M. S. 2012. Computer Networks and Internets: with Internet Applications, 4th Ed. India: Pearson Education.
3. Pahlavan, K. and Krishnamurthy, P. 2009. Networking Fundamentals: Wide, Local and Personal Area Communications. India: John Wiley & Sons.
4. Loo, J., Mauri, J. L. And Ortiz, J. H. 2012. Mobile Ad-hoc Networks: Current Status and Future Trends. CRC Press, USA: Taylor & Francis Group.

Objective: This course is designed to provide the students with a basic understanding and experiential learning of operating system. The course also provides details of various Microsoft Windows and Linux/Unix based operating systems.

Unit 1**14 Hours**

Fundamentals of Operating System: Operating System Functions, OS structures, Processes: Process control, Process states, Interacting processes, Process Control Block. Job Scheduling Algorithms.

Unit 2**14 Hours**

Deadlocks: handling deadlocks, deadlock detection and resolution, deadlock avoidance.
Memory Management: contiguous memory allocation, non contiguous memory allocation, Memory partitioning: fixed and dynamic, paging, segmentation, virtual memory.

Unit 3**14 Hours**

Windows System: Concepts and tools, System Architecture, Process Threads, and Jobs, Windows Management Mechanisms - The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications.

Unit 4**14 Hours**

Linux Systems : history, design principles, Kernal Modules, Process Management, Scheduling, Memory Management, File Systems, Input and Output, Inter-process Communication, Network Structure, Security.

Text books:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, Operating System Concepts, John Wiley & Sons ,Inc., 9th Edition,2012,.
2. Mark E. Russinovich and David A. Solomon, "Microsoft® Windows® Internals- Part 1", 6th Edition, Microsoft Press, 2012.
3. William Stallings, "Operating Systems: Internals and Design Principles", 7th Edition, Prentice Hall, 2012.

Suggested readings:

3. Mark E. Russinovich and David A. Solomon, "Microsoft® Windows® Internals- Part 2", 6th Edition, Microsoft Press, 2012.
4. Christopher Negus and Christine Breshnahan, "Linux Bible ", 8th Edition, John Willey & Sons, Inc., 2012.

CBS.505 Advanced Data Structures and Algorithms - Lab Credit Hour: 2

Students should be asked to implement the following algorithms in C/C++:

- Sorting Algorithms: Quick sort, Insertion Sort, Merge Sort.
- Greedy Algorithm to solve 0/1 knapsack problem
- Dynamic programming based algorithm to solve Matrix Chain Multiplication algorithm.
- Backtracking based algorithm to solve 8 Queen's problem
- Searching and Insertion operations on
 - Hash Tables,
 - Binary search Trees,
 - AVL Trees and
 - B-Trees,
- Pattern Matching Algorithms
 - Brute Force search algorithm
 - Boyer –Moore algorithm
 - Knuth-Morris-Pratt algorithm
- Algorithm for operation applicable on Tries and Priority Queues
- Any Practical related to other topics mentioned in theory syllabus

CBS.506 Advanced Computer Networks Lab Credit Hours: 2

In this practical class students should be asked to implement following scenarios in (Opnet/NS-2/NS-3) network simulator.

- Introduction and installation of Network Simulator.
- Introduction to Syntax, looping, conditional check, functions, execution of Mathematical Operations and Execution in Simulator.
- To study Nodes Creation, traffic flows, queuing disciplines and result analysis in network Simulator.
- To Simulate a Wired topology of multiple nodes.
- To explore the behaviour of TCP and UDP in both wired networks.
- To create Output files for analyzing and plotting received traffic/data.
- To Simulate a Wireless topology of multiple nodes.
- To analyze the performance of various routing protocols in a simulated environment.
- Any Practical related to other topics mentioned in theory syllabus

CBS.507 Seminar 1 Credit Hour: 2

The students should be asked to give seminar on advanced topic/case study/technology/tool in the field of cyber security. The purpose of the Seminar is to judge the knowledge of the students in field of cyber security and to discuss current trends in the field.

SEMESTER 2

CBS.508

Information Security

Credit Hours: 4

Objective: The main goal of this course is to provide background, foundation and insight into the many dimensions of information security. The primary objective is to understand information security's importance in increasingly computer-driven world.

Unit 1

14 Hours

Introduction: Meaning of Security, Attacks, Computer Security, Criminals, Methods of Defense, Encryption; Cryptography: Substitution Ciphers, Transpositions, Encryption Algorithms, Symmetric Encryption: Data Encryption Standards (DES), Advanced Encryption Standards (AES), Public Key Encryption, Hash Functions, Key exchange, Digital Signatures, Certificates.

Unit 2

14 Hours

Program Security: Non-malicious Program Errors, Viruses and Malicious Code: Malicious Code, Kinds of Malicious Code, Document Viruses, Virus Signatures, Sources of Virus, Preventing Virus Infection; Targeted Malicious Code, Controls against Program Threats.

Unit 3

14 Hours

Operating Systems Security: Protected Objects and Methods of Protection, Protecting Memory and Addressing, Protecting Access, File Protection Mechanisms, User Authentication, Trusted Operating Systems: Security Policies, Models of Security, Typical Operating System Flaws, Assurance Methods.

Unit 4

14 Hours

Database Security: Security requirements, Reliability and Integrity, Protecting sensitive data, Multilevel security.

Security Management: Personal Computer Security, Risk Analysis, Security Planning and Policies, Disaster Recovery.

Text books:

1. Pfleeger, C. P. and Pfleeger, S. L. 2003. Security in Computing, 3rd Ed, India: Pearson.
2. Stallings, W. 2010. Cryptography and Network Security. 5th ed Prentice Hall.

Suggested readings:

1. Forouzan, B.A. 2010. Cryptography & Network Security. McGraw-Hill Education.
2. Kahate, A. 2009. Cryptography and Network Security. McGraw-Hill Education.

Objective: The course is structured to understand fundamentals of Python Programming Language. The course also covers the use of Python Programming in Ethical Hacking/Network Security.

Unit 1**14 Hours**

Python Introduction, Installing and setting Python environment in Windows and Linux, basics of Python interpreter, Execution of python program, Editor for Python code, syntax, variable, types. Flow control: if, ifelse, for, while, range() function, continue, pass, break. Strings: Sequence operations, String Methods, Pattern Matching.

Unit 2**14 Hours**

Lists: Basic Operations, Iteration, Indexing, Slicing and Matrixes; Dictionaries: Basic dictionary operations; Tuples and Files; Functions: Definition, Call, Arguments, Scope rules and Name resolution;

Modules: Module Coding Basics, Importing Programs as Modules, Executing Modules as Scripts, Compiled Python files(.pyc), Standard Modules: OS and SYS, The dir() Function, Packages.

Unit 3**14 Hours**

Input output and file handling, Object Oriented Programming features in Python: Classes, Objects, Inheritance, Operator Overloading, Errors and Exceptions: try, except and else statements, Exception Objects, Regular expressions, Multithreading, Networking: Socket module.

Unit 4**14 Hours**

Role of Python in Hacking and Cyber Forensics, Debugging in python: introduction to PyDBG and immunity debugger; Hooking: Soft Hooking with PyDbg, Hard Hooking with Immunity Debugger, DLL and code injection: Remote Thread Creation, DLL Injection, Code Injection.

Text books:

1. Mark Lutz., 2009, "Learning Python",4th ed., O'REILLY Media, Inc..
2. Justin Seitz, 2009, "Gray Hat Python: Python Programming with Hackers and Reverse Engineers", No Starch Press, Inc.

Suggested readings:

1. Paul Berry, 2011, "Head First Python". O'REILLY Media, Inc.

Objective: This course offers a good understanding of network Investigation, web attack and DOS investigation and will prepare students to be in a position to perform network forensics. This course also helps to provide understanding of email system and tracking.

Unit 1**14 Hours**

Introduction to Network Forensics, Need of Cyber Forensics, Cyber Evidence: Incidents and Evident, Search and Seizure, Identification, Preservation, Analysis and Preparation, Documentation and Management of Crime Sense. Data image: Image Capturing and its importance, Partial Volume Image.

Unit 2**14 Hours**

Hidden Data Extraction: Data Hiding Techniques, Recovery of deleted files, Cracking Passwords, Data Extraction tools, Windows Registry Analysis, Network Forensics: Introduction to Network Forensics and Investigating Logs, Wired and Wireless Network Traffic capture and Analysis. Document Forensics: Information in Metadata.

Unit 3**14 Hours**

Web Attack Investigations: Introduction to Investigating Web Attacks, Indication of a Web Attack, Types of Web Attack. Denial of Service Investigations, Internet Crime Investigations: Introduction to Investigating Internet Crimes, Internet Forensics, Steps for Investigating Internet Crime.

Unit 4**14 Hours**

Email Crime Investigations: Email Structure, Email Addressing, Email Headers Analysis. Malware Forensics: Botnets, Automatic Self Updates, Fast Flux DNS, Network Behavior of Malware: Propagation, Command & Control, Payload Behaviour.

Text books:

1. Council, Ec. "Computer Forensics: Investigating Network Intrusions and Cybercrime", Cengage Learning. 2009.
2. Linda Volonino, "Computer Forensics for Dummies", Willey Publishing, Inc., 2012
3. Sherri Davidoff and Jonathan Ham, " Network Forensics Tracking Hackers through Cyberspace", Prentice Hall, 2012

Suggested readings:

1. Michael G. Solomon , K Rudolph, Ed Tittel, Neil Broom and Diane Barrett, "Computer Forensics Jump Start" 2nd Edition, Willey Publishing, Inc., 2011
2. Casey E., 2009. Handbook of Digital Forensics and Investigation, Academic Press.

CBS.511

Emerging Technologies

Credit Hours: 4

Objective: The objective of this course is to introduce emerging technologies in the field of Information technology. The security related issues in these technologies will also be discussed.

Unit 1

14 Hours

Grid Computing: Introduction to GRID Computing, How Grid Computing Works, Grid Middleware, Grid Architecture, Types of Grids, Grid Computing Applications, Technologies for Grid Computing, Clustering and Grid Computing, Issues in Data Grids, Key Functional Requirements in Grid Computing.

Unit 2

14 Hours

Cloud Computing : Introduction to Cloud Computing, Definition, Characteristics, Components, Cloud provider, SAAS, PAAS, IAAS and Others, Organizational scenarios of clouds, Administering & Monitoring cloud services, benefits and limitations, Comparison among SAAS, PAAS, IAAS Cloud security fundamentals, Privacy and Security in cloud, Cloud computing security architecture: Architectural Considerations-General Issues.

Unit 3

14 Hours

Mobile Computing: History of mobile communication, Types of Networks, Architecture for Mobile Computing, 3-tier Architecture, Design Considerations for Mobile Computing introduction to GSM system, GSM background, GSM operational and technical requirements. Cell layout and frequency planning, mobile station, base station systems, Security issues in mobile computing, Authentication, encryption.

Unit 4

14 Hours

Big Data: Introduction to Big Data, Big Data Tools and Techniques, Application of Big Data, Apache Hadoop, MapReduce, SMAQ Stack.

Text books:

1. Prabhu CSR, 2008, Grid and Cluster Computing, PHI.
2. Hurwitz J., Bloor R., Kanfman M., Halper F., 2010 Cloud Computing for Dummies, Wiley India.
3. William C.Y., Lee, 2010 Mobile Communication Design Fundamentals, John Wiley and Sons.
4. O'Reilly Media, Inc., 2012 Big Data Now, 2012 Edition, O'Reilly Media, Inc.

Suggested readings:

1. Krutz R. and Vines R.D., 2010, Cloud Security Wiley-India.
2. Schiller J., 2008, Mobile Communication, Pearson Education Asia.

CBS.512

Wireless LAN and Mobile Computing

Credit Hours: 4

Objective: The main objective of this course is to provide the students with the competences required for understanding and using the communications component of communications environment and to acquaint the students with basic knowledge and concepts of Wireless Data Transmissions.

Unit 1

14 Hours

Wireless Networks: Wireless Network, Wireless Network Architecture, Wireless Switching Technology, Wireless Communication problem, Wireless Network Reference Model, Wireless, Networking Issues & Standards.

Unit 2

14 Hours

Wireless LAN: Infra red Vs radio transmission, Infrastructure and Ad-hoc Network, IEEE 802.11: System Architecture, Protocol Architecture, 802.11b, 802.11a, Newer Developments, HIPERLAN 1, HIPERLAN 2, Bluetooth: User Scenarios, Architecture.

Global System for Mobile Communications (GSM): Mobile Services, System Architecture, Protocols, Localization & Calling, Handover, Security. GPRS: GPRS System, Architecture, UMTS: UMTS System Architecture. LTE: Long Term Evolution.

Unit 3

14 Hours

Mobile Computing: Mobile communication, Mobile computing, Mobile Computing Architecture, Mobile Devices, Mobile System Networks, Mobility Management, Mobile Network Layer: Mobile IP: Goals, Assumptions, Entities and Terminology, IP Packet Delivery, Agent Discovery, Registration, Tunneling and Encapsulation, Optimizations, Dynamic Host Configuration Protocol (DHCP)

Unit 4

14 Hours

Mobile Transport Layer: Traditional TCP, Indirect TCP, Snooping TCP, Mobile TCP, Fast retransmit/fast recovery, Transmission /time-out freezing, Selective retransmission, Transaction oriented TCP, TCP over 2.5G/3G Wireless Networks.

Text books:

1. Schiller, J. 2008. Mobile Communications. 2nd ed. India: Pearson Education.
2. Kumar, S. and Kakkasageri, M. S. "Wireless and Mobile Networks: Concepts and Protocols", Wiley India.
3. Kamal R. 2011. "Mobile Computing", 2nd Ed. Oxford University Press.

Suggested readings

1. Talukder, A. K., Ahmed, H. and Yavagal, R. R. 2010. Mobile Computing: Technology, Applications and Service Creation, 2nd Ed. Tata McGraw Hill.
2. Gast, M. S. "802.11 Wireless Networks: The Definitive Guide", O'Reilly Media.

Objective: The course is intended to provide with an understanding and solid technical overview of the database management systems.

Unit 1**14 Hours**

Introduction: File-Systems, database Approach, Database Environment, Database Languages, Data Models and Conceptual Modelling, Multi-user DBMS architecture, Relational Model and Languages: Relational Algebra and Calculus, SQL, Query-by-Example; Entity-Relationship Modeling, Enhanced Entity-Relationship Modeling, Normalization, Advanced Normalization.

Unit 2**14 Hours**

Database Issues: Database Security: Threats, Countermeasures, DBMS and Web Security; Transaction Management, Concurrency Control: Serializability & Recoverability, Locking Methods, Timestamping Methods; Database Recovery: Recovery Facilities and Techniques; Query Processing, Query Decomposition, Query Optimization.

Unit 3**14 Hours**

Distributed and Parallel DBMS: Distributed Database Concepts: Distributed Relational Database Design, Transparencies, Date's Twelve Rules, Distributed Transaction Management, Distributed Concurrency Control, Distributed Database Recovery, Distributed Query Optimization, Database Replication; Parallel DBMS Concepts: Interquery and Intraquery Parallelism, Interoperation and Intraoperation Parallelism.

Unit 4**14 Hours**

Object DBMS: Object-oriented Concepts, Object-oriented Database Design, Object-oriented Data Models, Object-oriented DBMSs, Issues in OODBMSs.

Data Warehousing and Data Mining: Evolution of Data Warehousing, Architecture, Data Flows, Tools & Technologies, Data Marts, Data Mining: Concepts, Techniques, Process, Tools.

Text books:

1. Connolly, T. and Begg, C. 2012. Database Systems, 4th Ed. India: Pearson Education.
2. Silberschatz, A. and Korth, H. F. and Sudarshan, S. 2011. Database System Concepts, 6th Ed. McGraw Hill.

Suggested readings:

1. Date, C. J., Kannan, A. and Swamynathan, S. 2012. An Introduction to Database Systems, 8th Ed. India: Pearson Education.
2. Elmarsi, R. and Navathe, S. B. 2013. Fundamentals of Database Systems, 5th Ed. India: Pearson Education.

The objective of this laboratory is to provide students research opportunity on data transmission security. The following lab exercises are based on the cryptographic algorithms. These can be implemented using C/C++/Java.

- To perform encryption and decryption using the following algorithms
 - Ceaser Cipher
 - Substitution Cipher
- To implement the Symmetric Encryption algorithms logic.
- To implement RSA Algorithm.
- To implement Diffie-Hellman Key Exchange Algorithm.
- To calculate the Message Digest of a text using different Message Digest algorithms.
- To implement wireless security protocols WEP/WPA/WPA2.
- Any Practical related to other topics mentioned in theory syllabus

CBS.515**Python Programming Lab****Credit Hour: 2**

In this practical session students should be asked to write programs in python using following concepts:

- Basic arithmetic operators,
- Flow Control and Iteration statements.
- Storing and processing data with strings,
- List and Dictionary: Creation and Manipulations.
- Tuples and Files
- Functions and arguments.
- Classes and Objects.
- Inheritance
- Operator Overloading
- Exception handling
- Python scripts for performing various hacks
 - DLL Injection
 - Code Injection
- Any Practical related to other topics mentioned in theory syllabus

CBS.516**Research Seminar****Credit Hour: 2**

The student shall have to write his synopsis including an extensive review of literature with simultaneous identification of scientifically sound (and achievable) objectives backed by a comprehensive and detailed methodology. The students shall also present their synopsis to the synopsis approval committee.

The Evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks
Review of literature	10
Identification of gaps in knowledge and Problem Statement	15
Objective formulation & Methodolgy	15
Presentation	10
Total	50

SEMESTER 3
Network Security

CBS.601

Credit Hours: 4

Objective: Upon completion of this course, participants will have gained knowledge of network security concepts: Authentication and security measures, understand Intrusion and filtering analysis techniques and key idea of VPN.

Unit 1

14 Hours

Network Perimeter Security Fundamentals: Introduction to Network Perimeter, Multiple layers of Network Security, Security by Router, Network Based Application Recognition.
Security Policy: Introduction, Force-able and Unforced-able policy, Elements of a policy, characteristics of a policy, User level policy, System level policy and Network Level Policy.

Unit 2

14 Hours

Firewalls: Firewall Basics, Types of Firewalls: Packet Filter, State-full Filter, Application Filter, Proxy Firewalls, Network Address Translation Issues, Linux IP Chains.
Access Control Lists: Ingress and Egress Filtering, Types of Access Control Lists, ACL types: standard and extended, ACL commands. CISCO IOS Basics, Tracking Rejected Traffic.

Unit 3

14 Hours

Network Intrusion Detection: Terminology, Comparison with firewalls, Anomaly based IDS, Signature based IDS, IDS sensor placement, Intrusion Prevention system.
Host Security: Host based IDS, Host Hardening, Role of Intelligent Techniques in Cyber Security & Intrusion Detection.

Unit 4

14 Hours

Virtual Private Networks: VPN Basics, Types of VPN, IPSec Tunneling, IPSec Protocols. VLAN: introduction to VLAN, VLAN Links, VLAN Tagging, VLAN Trunk Protocol (VTP). Wireless Network Security: Auditing and Securing Wireless Networks, Effective Wireless Architecture. Software Architecture and Network Defense, Software Architecture Issues.

Text books:

1. Riggs, C. 2005. Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA.
2. Northcutt S. 2005. Inside Network Perimeter Security, 2nd Ed., Pearson Education

Suggested readings:

1. Stallings W., 2010. Network Security Essentials (4th Edition), Prentice-Hall.

Objective: The objective of this course is to provide knowledge about the basic information on cyber law and also provide the basic information about amendment right and copyright issues. To understand ethical laws of computer for different countries this course also will be helpful.

Unit 1**14 Hours**

Introduction: Fundamentals of Cyber Space, Understanding Cyber Space, Interface of Technology and Law Defining Cyber Laws, Jurisdiction in Cyber Space, Concept of Internet Jurisdiction, Indian Context of Jurisdiction, International position of Internet Jurisdiction Cases in Cyber Jurisdiction.

Unit 2**14 Hours**

Specific issues: E-commerce- Legal issues, Legal Issues in Cyber Contracts, Cyber Contract and IT Act 2000, The UNCITRAL Model law on Electronic Commerce, Intellectual Property Issues and Cyberspace .

The Indian Perspective Overview of Intellectual, Property related Legislation in India Copyright law & Cyberspace, Trademark law & Cyberspace, Law relating to Semiconductor Layout & Design.

Unit 3**14 Hours**

Understanding Cyber Crimes: Defining Crime, Crime in context of Internet –Actus Rea/Mens Rea, Types of crime in Internet, Computing damage in Internet crime, Frauds: Hacking, Mischief, Trespass, Defamation, Stalking, Spam

Unit 4**14 Hours**

Obscenity and Pornography: Internet and Potential of Obscenity, Indian Law on Obscenity & Pornography, International efforts, Changes in Indian Law.

Penalties & Offences: IT Act 2001, Offences under the Indian Penal Code, Investigation & adjudication issues Digital evidence.

Text books:

1. Singh Y., 2012. Cyber Laws, 5th ed., Universal law Publishing Company.
2. Gupta A., 2011, Commentary on Information Technology Act, 2nd Ed.

Suggested readings:

1. Viswanathan A, 2012, Cyber Laws: Indian and International Perspectives on Key topics including Data Security, E-commerce, Cloud Computing and Cyber Crimes 1st Edition, LexisNexis

CBS.603**Network Security Lab****Credit Hour: 2**

The Network Security Lab tries to present several hands-on exercises to help reinforce the student's knowledge and understanding of the various network security aspects. In this practical session students should be asked to

- enable security over network by deploying access control list on router
- Implement Network based Application Recognition at CISCO router.
- Configure VLAN on managed layer 2 switches to provide isolation between various user groups.
- Deployment of Open sources Intrusion Detection system (SNORT)
- Configuration of Wireless LAN scenario.
- Implement firewall using IP Chain
- Analysis of network traffic using wire-shark.
- Any Practical related to other topics mentioned in theory syllabus

CBS.604**Seminar 2****Credit Hour: 2**

The students should be asked to give seminar on advanced topic/case study/technology/tool in the field of cyber security. The purpose of the Seminar is to judge the knowledge of the students in field of cyber security and to discuss current trends in the field.

CBS.605**Dissertation Part-1****Credit Hour: 12**

The objective of dissertation part-1 would be to ensure that the student learns the nuances of the scientific research. Herein the student shall have to carry out the activities/experiments to be completed during Dissertation Part-1 (as mentioned in the synopsis).

The students would present their work to the evaluation Committee (constituted as per the university rules). The Evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks	Evaluated By
Mid Term Report	100	Evaluation Committee
Presentation and defence of research work	100	
Continuous evaluation of student	100	Supervisor
Total	300	

SEMESTER 4

CBS.606

Ethical Hacking

Credit Hours: 4

Objective: This course will introduce basics of hacking. Various hacking techniques like Password hacking, TCP/IP hijacking, Wireless hacking and web hacking will be discussed in this course.

Unit 1

14 Hours

Introduction To Ethical hacking: Terminology, Ethical hacking versus auditing, Ethical hacking process, social engineering, Hackers behaviour & mindset, Maintaining Anonymity, Ethical Hacking Plan, Hacking Methodology, Information Gathering: Footprinting, Scanning & Enumeration.

Unit 2

14 Hours

Active and Passive Sniffing, Evasion: Intrusion Detection System & Firewall, Physical security vulnerabilities and countermeasures.

Windows Security Architecture, Hacking Windows based Operating System, Linux Security Architecture, Hacking Linux based operating systems, Password attacks, Privilege Escalation and Executing Applications, Social Engineering attacks and countermeasures.

Unit 3

14 Hours

Network Infrastructure Vulnerabilities, IP spoofing, port scanning, DNS spoofing, DOS attacks: SYN attacks, Smurf attacks, UDP flooding, DDOS – Models

Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Wireless network defence and counter measures, Gaining access (hacking 802.11), WEP, WPA, WPA2.

Unit 4

14 Hours

Web based hacking: Web server vulnerabilities, Web application vulnerabilities, Study of various attack: Input validation attacks, SQL injection attacks, Buffer overflow attacks

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metpreter, Introduction to Armitage.

Text books:

1. Matt Walker., All in One Certified Ethical Hacker Exam Guide, 2nd ed. Tata McGraw Hill Education.
2. Kevin Beaver, 2013, Hacking for Dummies, 3rd ed. John Wiley & sons.

Suggested readings:

1. McClure S., Scambray J., and Kurtz G, 2009, Hacking Exposed. Tata McGraw-Hill Education.

CBS.607**Ethical Hacking Lab****Credit Hour: 2**

In this practical session students should be asked to

- Perform footprint and collection of information about the system one need to hack.
- collect the network information by using network scanning tools such as nmap.
- Scan the remote system using vulnerability assessment tools such as openVAS.
- Perform Man-In –The – Middle-Attack using ARP poisoning.
- perform password cracking using tools such as Ophcrack.
- Scan vulnerabilities in wireless networks.
- bypass MAC filtering in Wireless LAN
- break WPA/WPA2 passwords
- Perform wireless Miss-association attack.

CBS.608**Seminar 3****Credit Hour: 2**

The students should be asked to give seminar on advanced topic/case study/technology/tool in the field of cyber security. The purpose of the Seminar is to judge the knowledge of the students in field of cyber security and to discuss current trends in the field.

CBS.609**Dissertation Part-2****Credit Hour: 16**

In Dissertation Part -2 the student shall have to carry out the activities/experiments to be completed during Dissertation Part-2 (as mentioned in the synopsis). The students would present their work to the evaluation Committee (constituted as per the university rules). The Evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks	Evaluated By
Final Report	150	Evaluation Committee
Presentation and defence of research work	150	
Continuous evaluation of student	100	Supervisor
Total	400	