MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB

Syllabus for B.Sc.in Cyber Security Programme

(Effective for Students Admitted in Academic Session 2019-2020)

Semester 4:

1. Cryptography & Information Security

UNIT I INTRODUCTION & NUMBER THEORY: Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid's algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat's and Euler's theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms. – 6L

UNIT II BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY: Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange-Elliptic curve arithmetic-Elliptic curve cryptography. – 8L

UNIT III HASH FUNCTIONS AND DIGITAL SIGNATURES: Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 – SHA – HMAC – CMAC – Digital signature and authentication protocols – DSS – EI Gamal – Schnorr. – 7L

UNIT IV SECURITY PRACTICE & SYSTEM SECURITY: Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security. – 7L

UNIT V E-MAIL, IP & WEB SECURITY: E-mail Security: Security Services for E-mail-attacks possible through E-mail – establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME. IPSecurity: Overview of IPSec – IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET). – 8L

Text :

1. "Cryptography and Network Security", William Stallings, 2nd Edition, Pearson Education Asia
2. "Network Security private communication in a public world", C. Kaufman, R. Perlman and M. Speciner, Pearson
3. Cryptography & Network Security: Atul Kahate, TMH.

Reference :

1. "Network Security Essentials: Applications and Standards" by William Stallings, Pearson
2. "Designing Network Security", Merike Kaeo, 2nd Edition, Pearson Books
3. "Building Internet Firewalls", Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, 2nd Edition, Oreilly
4. "Practical Unix & Internet Security", Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, Oreilly

2. Parallel and Distributed Computing

Introduction: Scope, issues, applications, and challenges of Parallel and Distributed Computing - 2L

Parallel Programming Platforms: Implicit Parallelism: Trends in Microprocessor Architectures, Dichotomy of Parallel Computing Platforms, Physical Organization, Communication Costs in Parallel Machines, Routing Mechanisms for Interconnection Networks, GPU, co-processing. – 4L

Principles of Parallel Algorithm Design: Decomposition Techniques,Characteristics of Tasks and Interactions,Mapping Techniques for Load Balancing. – 2L

CUDA programming model: Overview of CUDA, Isolating data to be used by parallelized code, API function to allocate memory on parallel computing device, to transfer data, Concepts of Threads, Blocks, Grids, Developing a kernel function to be executed by individual threads, Execution of kernel function by parallel threads, transferring data back to host processor with API function. – 6L

Analytical Modeling of Parallel Programs: Sources of Overhead in Parallel Programs, Performance Metrics for Parallel Systems, The Effect of Granularity on Performance, Scalability of Parallel Systems, Minimum Execution Time and Minimum Cost-Optimal Execution Time – 4L

Dense Matrix Algorithms: Matrix-Vector Multiplication, Matrix-Matrix Multiplication, Issues in Sorting on Parallel Computers, Bubble Sort and Variants, Quick Sort, Other Sorting Algorithms – 2L

Graph Algorithms: Minimum Spanning Tree: Prim's Algorithm, Single-Source Shortest Paths: Dijkstra's Algorithm, All-Pairs Shortest Paths, Transitive Closure, Connected Components, Algorithms for Sparse Graph Search Algorithms for Discrete Optimization Problems: Sequential Search Algorithms, Parallel Depth-First Search, Parallel Best-First Search, Speedup Anomalies in Parallel Search Algorithms – 6L

Cloud Computing: Introduction, Business Values, Inside Cloud Computing, Cloud Service Administration, Cloud Computing Technology, Accessing the Cloud, Data Management, Information Storage in Cloud Computing, Discovery of Private and Hybrid Clouds, Cloud Computing Standards, Migrating to the Cloud. – 10L

Books:

1. A Grama, A Gupra, G Karypis, V Kumar. Introduction to Parallel Computing (2nd ed.). Addison Wesley, 2003.
2. C Lin, L Snyder. Principles of Parallel Programming. USA: Addison-Wesley Publishing Company, 2008.
3. J Jeffers, J Reinders. Intel Xeon Phi Coprocessor High-Performance Programming. Morgan Kaufmann Publishing and Elsevier, 2013.
4. T Mattson, B Sanders, B Massingill. Patterns for Parallel Programming. Addison-Wesley Professional, 2004.

3. Ethical Hacking and Systems Defence – Certification

Module 1: Software and System Security
Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis (static, concolic and dynamic analysis), Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing. [6]

Module 2: Network Security & Web Security
Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP,, IPsec, BGP Security, DNS Cache poisoning etc), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Intrusion Detection tools, Threat Models, Denial of Service Attacks, DOS-proof network architecture, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security – Cross Site Scripting Attacks, Cross Site Request Forgery, SQL Injection Attacks, Content Security Policies (CSP) in web, Session Management and User Authentication, Session Integrity, Https, SSL/TLS, Threat Modeling, Attack Surfaces, and other comprehensive approaches to network design for security. [10]

Module 3: Security in Mobile Platforms
Android and ioS security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection. [4]

Module 4: Introduction to Hardware Security, Supply Chain Security
Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks. [4]

Module 5: Issues in Critical Infrastructure and SCADA Security
Security issues in SCADA, IP Convergence Cyber Physical System Security threats, Threat models in SCADA and various protection approaches, Machine learning and SCADA Security. [5]

Text Books

1. Web Application Security: Exploitation and Countermeasures for Modern Web Applications 1st Edition by Andrew Hoffman.
2. Software Security Vulnerability A Complete Guide - 2020 Edition Paperback – February 2, 2020 by Gerardus Blokdyk.
3. Pragmatic Software Security: A Practical Guide to Maturing Software Security One month at a time by Stephen M Dye
4. Software-Defined Networking and Security 1st Edition by Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody.
5. Managing the Security of Mobile Devices in the Enterprise By the National Institute of Standards and Technology.
6. Android Security: Attacks and Defenses By Anmol Misra and Abhishek Dubey
7. Android Security Internals: An In-Depth Guide to Android's Security Architecture By Nikolay Elenkov.
8. Practical Mobile Forensics – Third Edition: A Hands-On Guide to Mastering Mobile Forensics for the iOS, Android, and the Windows Phone Platforms By Rohit Tamma, Oleg Skulkin, Heather Mahalik, and Satish Bommisetty.
9. Hardware Security 1st Edition A Hands-on Learning Approach by Swarup Bhunia Mark Tehranipoor
10. Supply Chain Security: A Comprehensive Approach 1st Edition by Arthur G. Arway
11. Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems by Eric D. Knapp, Joel Thomas Langill
12. Handbook of SCADA/Control Systems Security, Second Edition by Robert Radvanovsky, Jacob Brodsky.

4. Software Engineering & software design with UML

Module I: Software Engineering –Objectives, Definitions, Software Process models - Waterfall Model, Prototype model, RAD, Evolutionary Models, Incremental, Spiral. Software Project Planning- Feasibility Analysis, Technical Feasibility, Cost- Benefit Analysis, COCOMO model. - 8L

Module II: Structured Analysis, Context diagram and DFD, Physical and Logical DFDs, Data Modelling, ER diagrams, Software Requirements Specification - 5L

Module III: Design Aspects: Top-Down and Bottom-Up design; Decision tree, decision table and structured English, Structure chart, Transform analysis Functional vs. Object- Oriented approach. Unified Modelling Language - Class diagram, interaction diagram: collaboration diagram, sequence diagram, state chart diagram, activity diagram, implementation diagram. – 7L

Module V: Coding & Documentation – Structured Programming, Modular Programming, Module Relationship-Coupling, Cohesion, OO Programming, Information Hiding, Reuse, System Documentation. Testing – Levels of Testing, Integration Testing, System Testing. 10L
Software Quality, Quality Assurance, Software Maintenance, Software Configuration Management, Software Architecture. – 6L

Books:

1. Software Engineering: A practitioner's approach– Pressman (TMH)
2. Software Engineering- Pankaj Jalote (Wiley-India)
3. Software Engineering- Rajib Mall (PHI)
4. Software Engineering –Agarwal and Agarwal (PHI)

5. Advanced computer network & Security

Unit I: Introduction: Introduction to Layered architecture, Networking hardware and software stacks.

Unit II: Network Performance: Network Simulation and Modelling, Performance issues in networks, Protocol case studies (e.g. HTTP, HTTPS, SSL, DHCP, DNS, Transport protocols and Routing protocols in wired and wireless networks and their performance).

Unit III: Modern Networks: Mobile Networks, Wireless Network, Sensor Networks, Vehicular Networks, Underwater Networks and Body Area networks and related performance issues.

Unit IV: Enterprise Networks: Enterprise network infrastructure planning and design. Capacity planning of servers and data centres.

Text Books:
1. B. A. Forouzan – "Data Communications and Networking (3rd Ed.) " – TMH
2. A. S. Tanenbaum – "Computer Networks (4th Ed.)" – Pearson Education/PHI
3. W. Stallings – "Data and Computer Communications (5th Ed.)" – PHI/ Pearson Education
4. Zheng & Akhtar, Network for Computer Scientists & Engineers, OUP
5. Black, Data & Computer Communication, PHI
6. Miller, data Communication & Network, Vikas
7. Miller, Digital & Data Communication, Jaico
8. Shay, Understanding Data Communication & Network, Vikas

Reference Books:
1. Kurose and Rose – " Computer Networking -A top down approach featuring the internet" – Pearson Education
2. Leon, Garica, Widjaja – "Communication Networks" – TMH
3. Walrand – "Communication Networks" – TMH.
4. Comer – "Internetworking with TCP/IP, vol. 1, 2, 3(4th Ed.)" – Pearson Education/PHI

Cryptography & Information Security Lab:

Experiments with -

1. Ceaser Cipher Encryption/Decryption
2. Monoalphabetic Encryption/Decryption
3. Polyalphabetic Cipher
4. PlayfairCipher
5. Hill Cipher
6. Diffie Hellman Key Exchange
7. RSA Encryption Decryption
8. Triple-DES Encryption Decryption

Case Study: Digital Signature
Case Study: Java Security Features/ Matlab Security Features
Case Study: Authentication in Kerbos

Software Engineering & software design with UML Lab

1.Preparation of requirement document for standard application problems in standard format. (e.g Library Management System, Railway Reservation system, Hospital management System, University Admission system)
2.Project Schedule preparation.
3. Use Case diagram, Class diagram, Sequence diagram and prepare Software Design Document using tools like Rational Rose. (For standard application problems)
4.Estimation of project size using Function Point (FP) for calculation.
5.Design Test Script/Test Plan (both Black box and White Box approach)
6.Compute Process and Product Metrics (e.g Defect Density, Defect Age, Productivity, Cost etc.)>Also by Cost Estimation models.

Advanced computer network & Security Lab

1. Configuration and logging to a CISCO Router and introduction to the basic user Interfaces. Introduction to the basic router configuration and basic commands.
2. Configuration of IP addressing for a given scenario for a given set of topologies.
3. Configure a DHCP Server to serve contiguous IP addresses to a pool of four IP devices with a default gateway and a default DNS address. Integrate the DHCP server with a BOOTP demon to automatically serve Windows and Linux OS Binaries based on client MAC address.
4. Configure, implement and debug the following: Use open source tools for debugging and diagnostics.
    a. ARP/RARP protocols
    b. RIP routing protocols
    c. BGP routing
    d. OSPF routing protocols
    e. Static routes (check using netstat)
5. Configure DNS: Make a caching DNS client, and a DNS Proxy; implement reverse DNS and forward DNS, using TCP dump/Wireshark characterise traffic when the DNS server is up and when it is down.
6. Configure FTP Server on a Linux/Windows machine using a FTP client/SFTP client characterise file transfer rate for a cluster of small files 100k each and a video file of 700mb.Use a TFTP client and repeat the experiment.
7. Configure a mail server for IMAP/POP protocols and write a simple SMTP client in C/C++/Java client to send and receive mails.
8. Implement Open NMS+ SNMPD for checking Device status of devices in community MIB of a Linux PC. Using yellow pages and NIS/NFS protocols implement Network Attached Storage Controller (NAS).Extend this to serve a windows client using SMB. Characterise the NAS traffic using wireshark.
9. Configure wirless network with AP, PC, Mobile Device.