M.D. UNIVERSITY, ROHTAK

SCHEME OF STUDIES AND EXAMINATION

B.Tech. CSE with Specialization Cyber Security)

Scheme effective from 2022-23

COURSE CODE AND DEFINITIONS

Course Code	Definitions
L	Lecture
P	Practical
LC	Laboratory Courses
PCC	Program Compulsory Course.
PEC	Program Elective Course
OE	Open Elective

NOTE: The minor has to be a subject offered by a department other than the department that offers the major of the student or it can be a different major offered by the same department. For example, a student with the declared major in Mechanical Engineering may opt to do a minor in CSE; in which case, the student shall receive the degree B.Tech., Mechanical Engineering with a minor in CSE. A student can do Majors in the chosen field as per the career goal, and a minor may be chosen to enhance the major thus adding diversity, breadth, and, enhanced skills in the field.

Advantages of Minor in Engineering:

The minors mentioned above are having lots of advantages and a few are listed below:

- To apply the interdisciplinary knowledge gained through a Major (Stream) + Minor.
- To enable students to pursue allied academic interests in contemporary areas.
- To provide an academic mechanism for fulfilling the multidisciplinary demands of industries.
- To provide effective yet flexible options for students to achieve basic to intermediate level competence in the Minor area.
- Provides an opportunity for students to become entrepreneurs and leaders by taking a business/management minor.
- Combination in the diverse engineering fields, e.g., ECE (Major) + Cyber Security (Minor) combination, increases placement prospects in various organizations seeking a combination of both skills.
- Provides an opportunity to Applicants to pursue higher studies in an interdisciplinary field of study.
- Provides an opportunity to the Applicants to pursue interdisciplinary research.
- To increase the overall scope of undergraduate degrees.

MAHARSHI DAYANAND UNIVERSITY, ROHTAK

SCHEME OF STUDIES & EXAMINATIONS
B.TECH. CSE with Specialization Cyber Security
w.e.f. 2022-2023

S. No.	Semester	Course Code	Course Title	Teaching Schedule			Internal Assesment	Examination Marks		Total	Credit	Duration of Exam
				L	T	P		Theory	Practical			
1	3rd Sem	PEC-CSE-001-F	E-Commerce and Cyber Laws	0	0	2	25	25	-	100	3	3
2	4th Sem	PEC-CSE-002-F	System and Network Security	3	0	0	25	75	-	100	3	3
3	5th Sem	PEC-CSE-003-F	Ethical Hacking	3	0	-	25	75	-	100	3	3
4.	5th Sem	PEC-CSE-004-F	Digital Forensics and Incident Response	0	0	2	25	75		100	3	3
5.	6th Sem	PEC-CSE-005-F	Cyber Space Operations and Design	3	0	0	25	75	-	100	3	3
6,	6th Sem	PEC-CSE-330G	Communication Engineering	3	0	2	25	75		100	3	3
7	7th Sem	PEC-CSE-415-G	Cyber Security Threats	3	0	0	25	75	-	100	3	3
8	7th Sem	**PEC-CSE-411-G**	Network Security and Cryptography	3	0	2	25	75		100	3	3
		Total								800	24	

E-Commerce and Cyber Laws

Course code	PEC-CSE-001-F				
Category	Professional Core Course				
Course title	E-Commerce and Cyber Laws				
Scheme and Credits	L	T	P	Credits	Semester-3
	3	0	0	3	
Branches (B. Tech.)	Computer Science and Engineering (minor in Cyber Security)				
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Unit-1

Electronic Commerce: Overview, Definitions, Advantages & Disadvantages of E-Commerce, Threats of E-Commerce, Cyber Laws. Technologies: Relationship between E-Commerce and Networking, Different Types of Networking for E-Commerce, internet, intranet, EDI Systems. Wireless Application Protocol: Definition, Hand Held Devices, Mobility & Commerce. Mobile Computing, Wireless Web, Web Security, Infrastructure Requirement for E-Commerce. Business Models of E-Commerce; Model Based on Transaction Type, Model Based on transaction Party – B2B, B2C, C2B, C2C, E-Governance.

Unit-2

Convergence: Technological Advances in Convergence – Types, Convergence and its implications, Convergence and Electronic Commerce. Collaborative Computing: Collaborative product development, Content Management: Definition of content, Authoring Tools and Content Management, Content – partnership, repositories, convergence, providers Web Traffic & Traffic management: Content Marketing. Call Centre: Definition, Need, Tasks Handled, Mode of Operation, Equipment, Strength & Weaknesses of Call Centre, Customer Premises Equipment (CPE). Supply Chain Management: E-logistics, Supply Chain Portal, Supply Chain planning Tools (SCP Tools), Supply Chain Execution (SCE), SCE – Framework, Internet 's effect on Supply Chain Power.

Unit– 3

E-Payment Mechanism; Payment through a card system, E-Cheque, E-Cash, E-Payment Threats & Protections, E-Marketing: Home – shopping, E-Marketing, Tele-Marketing Electronic Data Interchange (EDI): Meaning, Benefits, Concepts, Application, EDI Model, protocols (UN EDI FACT / GTDI, ANSIX – 12 Risk of E-Commerce: Overview, Security for E-Commerce, Security Standards, Firewall, Cryptography, Key Management, Password Systems, Digital Certificates, Digital Signatures

Unit-4

Enterprise Resource Planning (ERP): Features, capabilities, and Overview of Commercial Software, re-engineering work processes for IT applications, Business Process Redesign, Knowledge Engineering, and Data Warehouse. Business Modules: Finance, Manufacturing (Production), Human Resources, Plant Maintenance, Materials, Management, Quality Management Sales & Distribution ERP Package ERP Market: ERP Market Place, SAP AG, People Soft, BAAN, JD Edwards, Oracle Corporation. AI(Enterprise application integration)

System and Network Security

Course code	PEC-CSE-002-F				
Category	Professional Core Course				
Course title	System and Network Security				
Scheme and Credits	L	T	P	Credits	Semester-4
	3	0	0	3	
Branches (B. Tech.)	Computer Science and Engineering (minor in Cyber Security)				
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Objectives:
The purpose of this course is to provide an understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptops to large-scale infrastructures.

Learning Outcomes:
On completion of this course, students should have gained a good understanding of the concepts and foundations of computer security, and identify vulnerabilities of IT systems. The students can use basic security tools to enhance system security and can develop basic security enhancements in stand-alone applications.

Syllabus:

Unit-1:
Computer Security Concepts- Introduction to Information Security, Introduction to Data and Network Security, Integrity, and Availability, NIST FIPS 199 Standard, Assets and Threat Models, Examples
Control Hijacking– Attacks and defenses, Buffer overflow and control hijacking attacks Exploitation techniques and fuzzing- Finding vulnerabilities and exploits Dealing with Legacy code- Dealing with bad (legacy) application code: Sandboxing and Isolation.

Unit 2:
Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, Qmail, Chromium, and Android examples.
Basic web security model- Browser content, the Document object model (DOM), Same-origin policy. Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, The lock icon, User interface attacks, Pretty Good Privacy.

Unit 3:
Network Protocols and Vulnerabilities- Overview of basic networking infrastructure and network protocols, IP, TCP, Routing protocols, DNS.
Network Defenses- Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic: Denial of service attacks.
Malicious Software and Software Security- Malicious Web, Internet Security Issues, Types of Internet Security Issues, Computer viruses, Spyware, Key-Loggers, Secure Coding, Electronic and Information Warfare.

Unit 4:
Mobile platform security models- Android, ios mobile platform security models, Detecting Android malware in Android markets.
Security Risk Management- How Much Security Do You Really Need, Risk Management, Information Security Risk Assessment: Introduction, Information Security Risk Assessment, Case Studies, Risk Assessment in Practice.
The Trusted Computing Architecture- Introduction to Trusted Computing, TPM, Provisioning, Exact Mechanics of TPM.

Textbooks and References:

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

Ethical Hacking

Course code	PEC-CSE-003-F				
Category	Professional Core Course				
Course title	Ethical Hacking				
Scheme and Credits	L	T	P	Credits	Semester-5
	3	0	0	3	
Branches (B. Tech.)	Computer Science and Engineering (minor in Cyber Security)				
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objective:
Aim of this course is to teach students how to think like a hacker, providing them with a deep understanding of security issues and concerns. In addition, this course also provides the students with specialist knowledge and experience of advanced hacking techniques and their countermeasures.

Course Outcomes:

Upon completion of this course, the students will be able to:

- Critically evaluate the potential countermeasures to advanced hacking techniques.
- Analyze and critically evaluate techniques used to break into an insecure web application
- and identify relevant countermeasures.
- Demonstrate a critical evaluation of an advanced security topic with an independent project.

Syllabus:

Unit-1
Introduction: Understanding the importance of security, the Concept of ethical hacking and essential Terminologies-Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking, Foot printing, Scanning, System Hacking, and Session Hijacking.
Buffer Overflows Significance of Buffer Overflow Vulnerability, Why Programs/Applications are Vulnerability. Reasons for Buffer Overflow Attacks. Methods of ensuring that buffer overflows are trapped.

Unit-2

Sniffers: Active and passive sniffing. ARP poisoning and countermeasures. Man-in-the-middle attacks, Spoofing, and Sniffing attacks. Sniffing countermeasures.
SQL Injection: Attacking SQL Servers, Sniffing, Brute Forcing, and finding Application Configuration Files, Input validation attacks. Preventive Measures.

Unit-3
Web Application Threats, Web Application Hacking, Cross-Site Scripting / XSS Flaws / Countermeasures Correct Web Application Set-up.
Web Application Security: Core Defense Mechanisms. Handling User Access, Authentication, Session Management, Access Control.
Web Application Technologies: HTTP Protocol, Requests, Responses, and Methods. Encoding schemes. Server-side functionality technologies (Java, ASP, PHP).

Unit-4
Attacking Authentication: Attacking Session Management, Design Flaws in Authentication Mechanisms Attacking Forgotten Password Functionality, attacking Password change functions.
Countermeasures to authentication attacks Attacking other users: Reflected XSS Vulnerabilities, Stored XSS Vulnerabilities, DOM-Based XSS Vulnerabilities, HTTP Header Injection. Countermeasures to XSS.

Textbooks:
1. Patrick Engebretson, The Basics of Hacking and Penetration Testing, Elsevier, 2013.
2. Network Security and Ethical Hacking, Rajat Khare, Luniver Press, 2006.

Reference books:
1. Network intrusion alert: an ethical hacking guide to intrusion detection, Ankit Fadia, Manu Zacharia, Thomson Course Technology PTR, 2007.
2. Ethical Hacking, Thomas Mathew, OSB Publisher, 2003.
3. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and
George Kurtz, McGraw-Hill, 2005.

Digital Forensics and Incident Response

Course code	PEC-CSE-004-F				
Category	Professional Core Course				
Course title	Digital Forensics and Incident Response				
Scheme and Credits	L	T	P	Credits	Semester-5
	3	0	0	3	
Branches (B. Tech.)	Computer Science and Engineering (minor in Cyber Security)				
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objective:
Aim of this course is to teach deep understanding of security issues and digital forensics & incident response. In addition, this course also provides the students with specialist knowledge and experience of various digital forensics techniques and incident response.

Course Outcomes:

- Upon completion of this course, the students will be able to:
- Understanding of various digital forensics techniques and their usage for the potential
- countermeasures or incident response.
- Demonstrate a critical evaluation and use of digital forensics techniques to do incident
- response with an independent project.

Syllabus

Unit-1
Forensics Overview: Computer Forensics Fundamentals, Benefits of Computer Forensics, Computer Crimes, Computer Forensics Evidence and the Courts, Legal Concerns and Privacy Issues Forensics Process: Forensics Investigation Process, Securing the Evidence and Crime Scene, Chain of Custody, Law Enforcement Methodologies, Forensics Evidence, Evidence Sources.

Unit-2
Evidence Duplication, Preservation, Handling, and Security, Forensics Soundness, Order of Volatility of Evidence, Collection of Evidence on a Live System, Court Admissibility of Volatile Evidence

Unit 3
Acquisition and Duplication: Sterilizing Evidence Media, Acquiring Forensics Images, Acquiring Live Volatile Data, Data Analysis, Metadata Extraction, File System Analysis, Performing Searches, Recovering Deleted, Encrypted, and Hidden files, Internet Forensics, Reconstructing Past Internet Activities and Events, E-mail Analysis, Messenger Analysis: AOL, Yahoo, MSN, and Chats

Unit 4

Mobile Device Forensics: Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3. Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera, Court Testimony, Testifying in Court, Expert Witness Testimony, Evidence Admissibility

Text books:

- *Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics,*
- *McGraw-Hill Osborne Media, 3 rd editon, 2014.*
- *Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.*
-

Reference books:

- *John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital*
- *Forensics Paperback, February 24, 2012.*
- *Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and*
- *George Kurtz, McGraw-Hill, 2005.*

Cyber Space Operations and Design

Course code	PEC-CSE-005-F				
Category	Professional Core Course				
Course title	Cyber Space Operations and Design				
Scheme and Credits	L	T	P	Credits	Semester-6
	3	0	0	3	
Branches (B. Tech.)	Computer Science and Engineering (minor in Cyber Security)				
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objective:
This course provides a basic understanding of full-spectrum cyberspace operations, the complexities of the cyberspace environment, as well as planning, organizing, and integrating cyberspace operations. The course will consist of presentations and exercises that will teach students how to develop a cyber-operations design and bring it to fruition. At the conclusion of the course, students will have a fundamental understanding of how to analyze, plan for, and execute cyberspace operations.

Course Outcomes:
In this course, students will gain a better understanding of cyber operations (CO) for the deployment of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE), against an adversary to achieve objectives and cause effects in support of a mission set. This course, founded on concept operations and real cyber capabilities, provides students with the understanding, tools, and processes needed to conduct malware analysis with real-world malicious code samples to dissect. Students will be able to prepare and plan an effective offensive and defensive strategy, as well as evaluate covert protocols. Analysis of system-specific, non-descript tools will be introduced to aid in attack and defense.

Syllabus

Unit-1
Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, Developing a design approach, Planning for cyberspace operation

Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros, and cons of the different approaches

Unit-2
Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations.

Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise

Unit 3

Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber-workforce from senior leadership to the technical workforce

Unit-4

Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.

Textbooks and References:

- Paulo Shakarian et al. “Introduction of Cyber Warfare: A Multidisciplinary Approach,” syngress, Elsevier 2013.
- Jeffery carr et al, “Inside Cyber Warfare: Mapping the Cyber Underworld,” O’Reilly Publication December 2012.
- Jason Andress et al. “Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners” Syngress, Elsevier 2013.
- R. A. Clarke, Robert Knake “Cyber War: The Next Threat to National Security and What to Do About It” Haper Collins Publisher 2010.

Communication Engineering

Course code	PEC-CSE-330G (Common with ECE)				
Category	Program Core Course				
Course title	Communication Engineering				
Scheme and Credits	L	T	P	Credits	
	3	0	0	3	
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objective:

1. The course will give students about depth knowledge of the communication system.
2. To introduce students to random process and fundamental theorems
3. To make awareness of information theory and coding techniques

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 6 parts of 2.5 marks each from all units and remaining eight questions of 15 marks each to be set by taking two questions from each unit. The students have to complete five questions, first being compulsory and selecting one from each unit.

Unit:1
SPECTRAL ANALYSIS:
Fourier series, Fourier transforms, Convolution Theorem, Correlation, Cross-Correlation and autocorrelation.

Unit: 2
INFORMATION THEORY:
Introduction to information and entropy, channel capacity for discrete and continuous channels, Shannon's Theorem, Shannon-Hartley Theorem, Noisy channels, coding theory : Shannon-Fano coding, minimum redundance coding, maximization of entropy of a continuous message transmission rate, effect of medium on the information, selection of channels ,effect of noise and its minimization.

Unit:3
RANDOM SIGNAL THEORY:
Representation of random signals, concept of probability, probability of joint occurrence, conditional probability, discrete probability theory, continuous random variables, probability distribution function, probability density function, joint probability density functions.

Unit:4
RANDOM SIGNAL THEORY:

Statistical average and moments, Ergodic processes, correlation Function, power spectral density, central limit theory, response of the linear system to random signals. Error function Covariance relation among the spectral densities of the two input-output random processes. Cross spectral densities, optimum filters. Introduction to Linear Block Code and cyclic Codes

TEXTBOOK :
1. Principles of Communication Systems: Taub Schiling; TMH
REFERENCE BOOKS.
1. Communication Systems: Singh and Sapre ; TMH
2. Communication Systems: A Bruce Carlson; TMH

COURSE OUTCOMES: After the completion of the course the student will be able to:

- To Study and Derive equations for entropy mutual information and channel capacity for all types of channels.
- To acquire the knowledge about Fourier series and Fourier transform signal analysis tools.
- Design a digital communication system by selecting appropriate error-correcting codes for a particular application.
- To learn about the Probability of Random signal theory and process.
- Formulate the basic equations of linear block codes and a cyclic code.
- Compare the performance of digital communication system by evaluating the probability of error for different error correcting codes

Cyber Security Threats

Course code	PEC-CSE-415G				
Category	Professional Elective Course				
Course title	Cyber Security Threats				
Scheme and Credits	L	T	P	Credits	Semester 7
	3	0		3	
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objectives:

1. The learner will gain knowledge about securing both clean and corrupted systems, protect personal data, and secure computer networks.
2. The learner will understand key terms and concepts in cyber law, intellectual property and cybercrimes, trademarks and domain theft.
3. The learner will be able to examine secure software development practices.
4. The learner will understand principles of web security.
5. The learner will be able to incorporate approaches for risk management and best practices.
6. The learner will gain an understanding of cryptography, how it has evolved, and some key encryption techniques used today.
7. The learner will develop an understanding of security policies (such as confidentiality, integrity, and availability), as well as protocols to implement such policies.

Course Outcomes:

1. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure.
2. Design, develop, test, and evaluate secure software.
3. Develop policies and procedures to manage enterprise security risks.
4. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities, and training.
5. Interpret and forensically investigate security incidents.

Syllabus

UNIT 1

Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats – Web threats - Intruders and Hackers, Insider threats, Cybercrimes. Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms –Virus – Spam – Adware - Spyware – Trojans and covert channels – Backdoors – Bots – IP, Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats Environmental threats - Threats to Server security.

UNIT 2

Security Threat Management: Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness - Vulnerability sources and assessment- Vulnerability assessment tools – Threat identification - Threat Analysis - Threat Modelling - Model for Information Security Planning.

UNIT 3

Security Elements: Authorization and Authentication - types, policies and techniques – Security certification - Security monitoring and Auditing - Security Requirements Specifications – Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots

UNIT 4

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors – Security awareness, training, Email and Internet use policies.

Reference Books:

1. Swiderski, Frank and Syndex, “Threat Modeling”, Microsoft Press, 2004.
2. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, Prentice Hall, 2008.
3. Joseph M Kizza, “Computer Network Security”, Springer Verlag, 2005
4. Thomas Calabres and Tom Calabrese, “Information Security Intelligence: Cryptographic Principles & Application”, Thomson Delmar Learning, 2004.

Network Security and Cryptography

Course code	PEC-CSE-411G				
Category	Professional Elective Course				
Course title	Network Security and Cryptography				
Scheme and Credits	L	T	P	Credits	Semester 7
	3	0		3	
Class work	25 Marks				
Exam	75 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Objectives:

1. To understand cryptography theories; algorithms & systems.
2. To understand the symmetric and asymmetric key algorithms.
3. To understand necessary approaches & techniques to build protection mechanisms in order to secure Computer Networks.
4. Acquire fundamental knowledge on the concepts of different security layers.

Course Outcomes:

After completing the course, the student will be able to

- Compare various cryptographic techniques.
- Work with symmetric & asymmetric key algorithms.
- Design secure applications.
- Inject secure coding in the developed applications.

Syllabus

UNIT- I

Introduction: Plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography.

UNIT- 2

Symmetric Key Algorithms: - Introduction, algorithms types, and modes, DES, AES.

Asymmetric Key Algorithms: Introduction, history of asymmetric key cryptography, RSA symmetric and asymmetric key cryptography together, Digital signature.

UNIT- 3

Internet Security Protocols: Basic concepts, Secure Socket Layer (SSL), Transport Layer Security (TLS), Secure Hyper Text Transfer Protocol (SHTTP), Time Stamping Protocol (TSP), Secure Electronic Transaction (SET), S SL versus SET, Electronic Money, Email Security.

UNIT- 4

User Authentication And Kerberos:- Introduction, Authentication basics, Passwords, authentication tokens, certificate-based authentication, biometric-based authentication, Kerberos, key distribution center(KDC), Security handshake pitfalls, Single Sign-on(SSO) approach.

TEXT/ REFERENCE BOOKS:

1. Cryptography and Network Security, 2nd Edition by Atul Kahate, TMH
2. Network Management Principles & Practices by Subramanian, Mani (AWL)
3. SNMP, Stalling, Willian (AWL)
4. SNMP: A Guide to Network Management (MGH)
5. Telecom Network Management by H.H. Wang (MGH)
6. Network Management by U. Dlack (MGH)