

UNIVERSITY OF MUMBAI



Syllabus for
M. E. in Information Technology
with specialization in
Information and Cyber Warfare
Under
FACULTY OF TECHNOLOGY

(As per Credit Based Semester and Grading System
with effect from the academic year 2013–2014)

**Program Structure for
ME in Information Technology with specialization in
Information and Cyber Warfare
Mumbai University**

(With Effect from 2013-2014)

Semester I

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned						
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total			
ICW101	Computer Network and Design	04	--	--	04	--	--	04			
ICW 102	Information Theory	04	--	--	04	--	--	04			
ICW 103	Web Application Hacking I	04	--	--	04	--	--	04			
ICW 101X	Elective I	04	--	--	04	--	--	04			
ICW 102X	Elective II	04	--	--	04	--	--	04			
ICW 101L	Laboratory I	--	02	--	--	01	--	01			
ICW 102L	Laboratory II	--	02	--	--	01	--	01			
Total		20	04	--	20	02	--	22			
Subject Code	Subject Name	Examination Scheme									
		Theory					End Sem. Exam	Exam Duration (hr)	Term Work	Pract. /oral	Total
		Internal Assessment			Test 1	Test 2					
		Test 1	Test 2	Avg.							
ICW 101	Computer Network and Design	20	20	20	80	3	--	--	100		
ICW 102	Information Theory	20	20	20	80	3	--	--	100		
ICW 103	Web Application Hacking I	20	20	20	80	3	--	--	100		
ICW 101X	Elective I	20	20	20	80	3	--	--	100		
ICW 102X	Elective II	20	20	20	80	3	--	--	100		
ICW 101L	Laboratory I	--	--	--	--		25	25	50		
ICW 102L	Laboratory II	--	--	--	--		25	25	50		
Total		100	100	100	400		50	50	600		

Semester II

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned						
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total			
ICW 201	Network Security	04	--	--	04	--	--	04			
ICW 202	Cyber Law	04	--	--	04	--	--	04			
ICW 203	Cryptography and PKI	04	--	--	04	--	--	04			
ICW 201X	Elective III	04	--	--	04	--	--	04			
ICW 202X	Elective IV	04	--	--	04	--	--	04			
ICW 203L	Laboratory III	--	02	--	--	01	--	01			
ICW 204L	Laboratory IV	--	02	--	--	01	--	01			
Total		20	04	--	20	02	--	22			
Subject Code	Subject Name	Examination Scheme									
		Theory					End Sem. Exam.	Exam Duration (hr)	Term Work	Pract. /oral	Total
		Internal Assessment			Avg .	Total					
Test1	Test 2	Avg .	End Sem. Exam.	Exam Duration (hr)			Term Work	Pract. /oral	Total		
ICW 201	Network Security	20	20	20	80	3	--	--	100		
ICW 202	Cyber Law	20	20	20	80	3	--	--	100		
ICW 203	Cryptography and PKI	20	20	20	80	3	--	--	100		
ICW 201X	Elective III	20	20	20	80	3	--	--	100		
ICW 202X	Elective IV	20	20	20	80	3	--	--	100		
ICW 203L	Laboratory III	--	--	--	--		25	25	50		
ICW 204L	Laboratory IV	--	--	--	--		25	25	50		
Total		100	100	100	400		50	50	600		

Semester III

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned				
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total	
ICWS301	Seminar	--	06	--	--	03	--	03	
ICWD301	Dissertation I	--	24	--	--	12	--	12	
Total		--	30	--	--	15	--	15	
Subject Code	Subject Name	Examination Scheme							
		Theory				End Sem.Exam.	Term Work	Oral.	Total
		Internal Assessment							
		Test1	Test 2	Avg.					
ICWS301	Seminar	--	--	--	--	50	50	100	
ICWD301	Dissertation I	--	--	--	--	100	--	100	
Total		--	--	--	--	150	50	200	

Semester IV

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned				
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total	
ICWD401	Dissertation II	--	30	--	--	15	--	15	
Total		--	30	--	--	15	--	15	
Subject Code	Subject Name	Examination Scheme							
		Theory				End Sem Exam	Term Work	Oral.	Total
		Internal Assessment							
		Test1	Test 2	Avg.					
ICWD401	Dissertation II*	--	--	--	--	100	100	200	
Total		--	--	--	--	100	100	200	

* The Term Work and Oral of Dissertation II of Semester IV should be assessed jointly by the pair of Internal and External Examiners

Note- The Contact Hours for the calculation of load of teacher are as follows

Seminar - 01 Hour / week / student

Dissertation I and II - 02 Hour / week / student

List of Elective Subjects

Subject Code	Elective I	Subject Code	Elective II
ICW1011	Mobile and Pervasive Computing	ICW 1021	Cloud Computing and Security
ICW 1012	Steganography and covert Communication	ICW 1022	Mobile Commerce and Security
ICW 1013	Web Application Security Testing	ICW 1023	Global Cyber Warfare

Subject Code	Elective III	Subject Code	Elective IV
ICW 2011	Information Security & Risk Management	ICW 2021	Storage Area Network
ICW 2012	Social Engineering and Reality mining	ICW 2022	Intrusion Detection Systems
ICW 2013	Web Application Hacking II	ICW 2023	Advanced Computer Forensic Analysis

End Semester Examination: In all six questions to be set, each of 20 marks, out of these any four questions to be attempted by students. Each question will comprise of mixed questions from different units of the subjects.

Semester I

Subject Code	Subject Name	Credits
ICW101	Computer Network and Design	04
Module	Detailed content	Hours
1	Internet Protocol (Configuration of DMZ Servers): Detail Working of DNS, HTTP, FTP and SMTP/POP - Configuration of DNS, Web, FTP, Mail Server. Internet Protocol – Understanding working of TCP, UDP, IP, ARP/ RARP, ICMP.	4
2	Introduction to Network analysis , Architecture and Design Process Model for Network analysis, Architecture, and Design	4
3	Requirement Analysis: User Requirement, Device Requirement, Network Requirement, Performance Requirement, Financial Requirement, Enterprise Requirement	4
4.	Network Architecture: Component Architecture –Routing, Network Management, Performance, Security. Architectural models: topological, flow model, Functional model Addressing And Routing Architecture, Network Management Architecture, Performance Architecture, Borderless Network Architecture, Data centre/	6
5	Network Design: Designing the network topology and solutions-Top down Approach Network Structure Model: Hierarchical Network Model, Enterprise wide network Architecture model- Enterprise Edge Area, E-commerce, Internet Connectivity, remote, enterprise branch and enterprise Data Center module. High Availability Network Services- Workstation to Router redundancy, and LAN High Availability protocols, Route Server	6
6	Enterprise LAN Design: Ethernet Design Rule. 100 Mbps Fast Ethernet Design rules, gigabit Ethernet Design Rules, 10 Gigabit Ethernet Design rules, 10GE Media types Understanding Working of Repeater, hub, Bridge, routers, Layer2/3 Switch Campus LAN Design Best Practice Server Farm Design, data centre Design Campus LAN QoS consideration Multicast Traffic Consideration.	6
7	Wireless LAN Design	2
8	WAN Technologies: WAN Transport Technologies, WAN Design Methodology, Traditional WAN Technologies, Remote Access Network Design, VPN Network Design, WAN Backup Design	2
9	Internet routing Protocol: IP Address Classful and CIDR, Private and Public IP address and NAT guidelines, IP Subnet Design, Routing Protocol, RIP, OSPF, Interior and Exterior Routing Protocol. BGP, IPV6 and IPV6 Routing Protocol	4
10	Network Management Prtocols: SNMP v1,v2,v3, RMON2, Netflow, Syslog	2

11	Network Analysis Queue Models: Arrival Processes, Service time Queuing System, Clarification M/M/1 Queue and basic multiplexer model M/M/1 state probabilities and notion of stability, effect of scale on performance, average packet delay via network, The M/G.I model,	4
----	--	---

Text Books :

1. Network Analysis, Architecture, and Design 3rd Edition, Morgan Kaufman, James D.
2. CCDA Cisco official Guide
3. Behrouz A. Forouzan: Data Communications and Networking, 4th Edition, Tata McGraw-Hill, 2006.

Reference Books:

1. Advanced Computer network; Ambavade, dreamtech
2. William Stallings: Data and Computer Communication, 8th Edition, Pearson Education, 2007.
3. Larry L. Peterson and Bruce S. David: Computer Networks – A Systems Approach, 4th Edition, Elsevier, 2007.
4. Wayne Tomasi: Introduction to Data Communications and Networking, Pearson Education, 2005.
5. Tamara's Network+ - Guide Networks, Second edition, published by Thomson Learning, 2002.
6. James F. Kuross, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet”, Third Edition, Addison Wesley, 2004.
7. Nader F. Mir, “Computer and Communication Networks”, Pearson Education, 2007.
8. Comer, “Computer Networks and Internets with Internet Applications”, Fourth Edition, Pearson Education, 2005.
9. Andrew S. Tanenbaum, “Computer Networks”, Sixth Edition, 2003, PHI Learning.
10. William Stallings, “Data and Computer Communication”, Sixth Edition, Pearson Education, 2000

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW102	Cryptography and PKI	04
Module	Detailed content	Hours
1	Cryptography: Concepts and Techniques: Introduction, Security Trends, Model for Network Security, Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key Size, Possible Types of Attacks	06
2	Symmetric Key Algorithms: DES, 3DES, AES, IDEA, RC4, RC5, Confidentiality using symmetric encryption.	04
3	Introduction to Number Theory: Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms Public- Key Cryptography and RSA: Principles of Public-Key Cryptosystems, RSA, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.	08
4	Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, MAC, Hash Functions, Security of Hash Functions and MACs, SHA, HMAC	05
5	Digital Signatures and Public Key Infrastructure (PKI): Digital Signatures, Authentication Protocols, DSS, Authentication Applications: Kerberos, X.509 Authentication Service Digital Certificates, Private Key Management, PKI Trust Models, Public Key Cryptography Standards, Revocation, Directories and PKI, PKIX and Security.	08
6	Elliptic Curves: The Addition Law, Elliptic curve Mod p, Factoring with Elliptic Curves, Elliptic Curve Cryptosystems	03
7	Cryptography in Java, .NET and Operating Systems: Cryptographic Solutions using Java, Cryptographic Solutions using Microsoft .NET Framework, Cryptographic Toolkits, Security and Operating Systems, Database Security.	06

Text Books:

1. Information Security Principal and Practice: Mark stamp, Wiley
2. Cryptography and security, wiley,Shyamala,harini

Reference Books:

1. Stallings, W., "Cryptography and Network Security", Fourth Edition, Pearson
2. Introduction to Cryptography with coding Theory, Pearson, WadenTrappe
3. Forouzan B., "Cryptography and Network Security", Second Edition, Tata McGraw Hill

4. Bernard Menezes, "Network Security and Cryptography", Cengage Learning.
5. Charlie Kaufman, Radia Perlman and Mike Speciner "Network security, private communication in a public world" , Second Edition, Pearson.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW103	Web Application Hacking I	04
Module	Detailed content	Hours
1	Web Application Insecurity and Defence Mechanism: The Evolution of Web Applications, Web Application Security ,Key Problem Factors , Handling User Access , Handling User Input,Handling Attackers	06
2	Web Application Technologies and Mapping Application : HTTP Protocol,Web Functionality,Encoding Schemes , Enumerating Content and Functionality , Analyzing Application	06
3	Attacking Authentication Authentication Technologies , Design Flaws in Authentication ,Implementation Flaws in Authentication , Securing Authentication	06
4	Attacking Session Management The Need for State ,Weaknesses in Token Generation, Weaknesses in Session Token Handling ,Securing Session Management	03
5	Attacking Access Controls Common Vulnerabilities ,Attacking Access Controls,Securing Access Controls	03
6	Attacking Data Stores Injecting into Interpreted Contexts, Injecting into SQL, Injecting into NoSQL ,Injecting into XPath, Injecting into LDAP .	03
7	Attacking Back-End Components Injecting OS Commands, Manipulating File Paths,Injecting into XML Interpreters ,Injecting into Back-end HTTP Requests ,njecting into Mail Services .	04
8	Attacking Application Logic The Nature of Logic Flaws, Real-World Logic Flaws, Ex1.Fooling a Password Change Function , Ex2.Breaking the Bank , Ex3. Cheating on Bulk Discounts , Ex.4.Invalidating Input Validation , Ex5.Racing Against the Login ,Avoiding Logic Flaws	06

Text Book:

1. Web Application Hackre’s Handbook, Dafydd Stuttarf, Marcus Pinto, Wiley

Reference Books:

2. Hacking Exposed Web Applications, 3rd Edition, by Joel Scambray, Vincent Liu and Caleb Sima.
3. Web Application Defender's Cookbook: Battling Hackers and Protecting Users by Ryan C. Barnett and Jeremiah Grossman

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should

be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1011	Mobile and Pervasive Computing	04

Module	Detailed content	Hours
1	Mobile Networks: Cellular Wireless Networks, GSM: Architecture, Protocols, Connection Establishment, Frequency Allocation, Routing, Mobility Management, Security, GPRS.	06
2	Wireless Networks: Issues and challenges of Wireless networks – Location management, Resource management, Routing, Power management, Security. Wireless Media Access Techniques – ALOHA , CSMA , Wireless LAN , MAN , IEEE 802.11 (a,b,e,f,g,h,i), Bluetooth, Wi-Fi, WiMAX Wireless routing protocols – Mobile IP, IPv4, IPv6, Wireless TCP. Protocols for 3G & 4G cellular networks – IMT – 2000, UMTS, CDMA2000, Mobility management and handover Technologies, All-IP based cellular network	06
3	Routing: Mobile IP, DHCP, AdHoc, Proactive and Reactive Routing Protocols, Multicast Routing. Mobile networks – Ad-hoc networks, Ad-hoc routing, Sensor networks, Peer-Peer networks. Mobile routing protocols – DSR, AODV, Reactive routing, Location aided routing. Mobility models – Entity based, Group mobility, Random Way-Point mobility model.	06
4	Transport And Application Layers: Mobile TCP, WAP, Architecture, WWW Programming Model, WDP, WTLS, WTP, WSP, WAE, WTA Architecture, WML, WMLScripts.	04
5	Pervasive Computing: Pervasive computing infrastructure, applications, Device Technology, Hardware, Human-machine Interfaces, Biometrics, and Operating systems, Device Connectivity, Protocols, Security, and Device Management, Pervasive Web Application architecture, Access from PCs and PDAs - Access via WAP	06
6	Mobile Software: Software adaptation and OS support. Resource sharing. OS for embedded devices: PalmOS, WindowsCE, Embedded Linux, WAP/WML, J2ME, Windows Mobile and .Net Framework, BREW. Mobile agents, Resource and service discovery, Mobile Java, Mobile GriJ and collaborative processing with Jini. Android Development	08
7.	Security Challenges in Pervasive computing.	04

Text Books:

1. Jochen Schiller, “Mobile Communications”, PHI.
2. Jochen Burkhardt, Pervasive Computing: Technology and Architecture of Mobile Internet Applications, Addison-Wesley Professional; 3rd edition, 2007

References:

1. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill

2. Debashis Saha, Networking Infrastructure for Pervasive Computing: Enabling Technologies, Kluwer Academic Publisher, Springer; First edition, 2002
3. Introduction to Wireless and Mobile Systems by Agrawal and Zeng, Brooks/ Cole (Thomson Learning).
4. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, Principles of Mobile Computing, Springer, New York, 2003
7. R. Riggs, A. Taivalsaari, M. VandenBrink, Programming Wireless Devices with Java2 Platform, Micro Edition, Addison-Wesley, 2001.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1012	Steganography and Covert Communication	04

Module	Detailed content	Hours
1	Introduction : Covert Communication, Steganography, Cryptography and Network Security , Types of Cryptography , Cryptography tools	04
2	Hiding with Steganography : Overview of Steganography, Variations on Stego, Security and Steganography, Principles of Steganography ,Types of Steganography ,	06
3	Digital Watermarking: Properties of Digital Watermarking ,Types of Digital watermarking , Goals of Digital Watermarking ,Digital Watermarking and Stego ,Uses of Digital Watermarking , Removing Digital Watermarks	06
4	Steganography at Large: Climate for Deceit, Corporate Espionage , Playing Spy , Information crimes and Law, Enforcement , Types of Steganography,New Classification Scheme , Color Tables ,Products That	06
5	Sending Stegano Files Across a Network : Uses and Techniques of Network Stego, Network Stego Techniques, Hiding in a transmission, Hiding Data in Network Headers, Hiding in an Overt Protocol	06
6	Cracking Stegano and Crypto : Identification, Cracking Analysis, Role of Detection, Cracking Cryptography, General Attacks, Specific Attacks, Cracking Steganography, General Techniques , Specific Techniques	06
7.	Developing Own Secure Communications Strategy: Secure versus Secret , Setting Communication Goals, Roles of Crypto and Stego in Business , Developing a Strategy ,Common Problems with Secure Technologies, New and Improved Ways to Use Stego	06

Text Book:

1. Eric Cole”Hiding in Plain Sight . Steganography and the Art of Covert Communication ”.

Reference Books:

1. Noiseless Steganography: The Key to Covert Communication by Abdelrahman Desoky, CRC Press.
2. Disappearing Cryptography: Information Hiding: Steganography & Watermarking by Peter Wayner, Third Edition.
3. Digital Watermarking and Steganography, 2nd Ed. (The Morgan Kaufmann Series in Multimedia Information and Systems) by Ingemar Cox, Matthew Miller, Jeffrey Bloom and Jessica Fridrich
4. Digital Watermarking and Steganography: Fundamentals and Techniques by Frank Y. Shih

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is

End Semester Examination: either a class test or assignment on live problems or course project. Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1013	Web Application Security Testing	04

Module	Detailed content	Hours
1	Open Web Application Security – Introduction, Top 10 Attacks, Information Gathering Search Engine Discovery/Reconnaissance Identify application entry points Testing for Web Application Fingerprint. Application Discovery, Analysis of Error Codes.	04
2	Configuration Management Testing: SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) , DB Listener Testing Infrastructure Configuration Management Testing) Application Configuration Management Testing, Testing for File Extensions Handling , Old, Backup and Unreferenced Files, Infrastructure and Application Admin Interfaces, Testing for HTTP Methods and Cross Site Tracing (XST).	06
3	Authentication Testing: Credentials transport over an encrypted channel , Testing for user enumeration , Testing for Guessable (Dictionary) User Account, Brute Force Testing, Testing for bypassing authentication schema, Testing for vulnerable remember password and pwd reset, Testing for Logout and Browser Cache Management, Testing for CAPTCHA, Testing Multiple Factors Authentication, Testing for Race Conditions.	06
4	Session Management Testing Testing for Session Management Schema, Testing for Cookies attributes, Testing for Session Fixation, Testing for Exposed Session Variables, Testing for Cross Site Request Forgery (CSRF).	04
5	Authorization Testing : Testing for path traversal, Testing for bypassing authorization schema, Testing for Privilege Escalation, Business Logic Testing.	04
6	Data Validation Testing: Testing for Reflected Cross Site Scripting, Testing for Stored Cross Site Scripting, Testing for DOM based Cross Site Scripting, Testing for Cross Site Flashing, Testing for SQL Injection, Oracle Testing, MySQL Testing, SQL Server Testing MS Access Testing, Testing PostgreSQL	06
7	Testing for Denial of Service Testing for SQL Wildcard Attacks, Testing for DoS Locking Customer Accounts , Testing for DoS Buffer Overflows, Testing for DoS User Specified Object Allocation, Testing for User Input as a Loop Counter, Testing for Writing User Provided Data to Disk, Testing for DoS Failure to Release Resources, Testing for Storing too Much Data in Session	06
8	Web Services Testing WS Information Gathering, Testing WSDL, XML Structural Testing, XML Content-level Testing, HTTP GET parameters/REST Testing, Naughty SOAP attachments, Replay Testing, AJAX Testing, AJAX Vulnerabilities , How to test AJAX	04

Reference books:

1. Open Web Application Security Project (OWASP): 2013
2. Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast, O'Reilley.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1021	Cloud Computing and Security	04
Module	Detailed content	Hours
1	Introduction to cloud computing, cloud architecture and service models, the economics and benefits of cloud computing, horizontal/vertical scaling, thin client, multimedia content distribution, multiprocessor and virtualization, distributed storage.	04
2	Federation/presence/ identity/privacy in cloud computing : Four Levels of Federation, Federated Services and Applications , Protecting and Controlling Federated Communication, Presence in the Cloud ,Presence Protocol, The Interrelation of Identity, Presence, and Location in Cloud , Federated Identity Management , Cloud and SaaS Identity Management ,Federating Identity , Privacy and Its Relation to Cloud-Based Information Systems , Privacy Risks and the Cloud , Protecting Privacy Information	08
3	free cloud services and open source software , and example commercial cloud services ,Cloud Computing and Virtualization ,Host Clusters ,Storage Virtualization, VM clusters ,Cloud security fundamentals, Vulnerability assessment tool for cloud, Privacy and Security in cloud	06
4	Cloud computing security architecture: Architectural Considerations-General Issues, Trusted Cloud computing, Secure Execution Environments and Communications, Micro-architectures; Identity Management and Access control-Identity management, Access control, Autonomic Security Cloud computing security challenges: Virtualization security management- virtual threats, VM Security Recommendations, VM-Specific Security techniques, Secure Execution Environments and Communications in cloud.	08
5	Cloud Platform Architectures : Amazon AWS, Microsoft Azure, Google App Engine, Google MapReduce / Yahoo Hadoop, Eucalyptus, Nimbus, OpenStack Common Standards in Cloud Computing: Distributed Management Task Force , Open Virtualization Format , Standards for Application Developers , Browsers (Ajax) ,Data (XML, JSON) , Solution Stacks (LAMP and LAPP) ,Standards for Messaging , Simple Message Transfer Protocol (SMTP) , Post Office Protocol (POP) , Internet Messaging Access Protocol (IMAP) , Syndication (Atom, Atom Publishing Protocol, and RSS) , Communications (HTTP, SIMPLE, and XMPP) ,Standards for Security , Security (SAML OAuth, OpenID, SSL/TLS)	06
6	Issues in cloud computing, Implementing real time application over cloud platform , Issues in Intercloud environments, QOS Issues in Cloud, Dependability, data migration, streaming in Cloud. Quality of Service (QoS) monitoring in a Cloud computing environment. Cloud Middleware. Mobile Cloud Computing. Inter Cloud issues. A grid of clouds, Sky computing, load balancing, resource optimization, resource dynamic reconfiguration, Monitoring in Cloud	08

Text Books:

1. Enterprise Cloud Computing by Gautam Shroff, Cambridge
2. Cloud Security by Ronald Krutz and Russell Dean Vines, Wiley-India

Reference Books:

1. Google Apps by Scott Granneman, Pearson
2. Cloud Security & Privacy by Tim Malhar, S.Kumaraswamy, S.Latif (SPD, O'REILLY)
3. Cloud Computing: A Practical Approach, Anthony T Velte, et.al McGraw Hill,
4. Cloud Computing Bible by Barrie Sosinsky, Wiley India
5. Cloud Computing Implementation, Management, and Security by John W. Rittinghouse
James F. Ransome
6. Stefano Ferretti et.al. "QoS-aware Clouds", 2010 IEEE 3rd International Conference on Cloud Computing

Assessment:**Internal:**

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1022	Mobile Commerce and Security	04

Module	Detailed content	Hours
1	<p>Introduction to M-commerce : Infrastructure Of M–Commerce, Types Of Mobile Commerce Services, Technologies Of Wireless Business, Benefits And Limitations, Support, Mobile Marketing & Advertisement, Non–Internet Applications In M–Commerce, Wireless/Wired Commerce Comparisons. Emerging applications, different players in m-commerce, m-commerce life cycle, M-commerce business models, The m-commerce value chain, M-commerce information system functional model. Case study</p>	06
2	<p>M-commerce technology: Mobile clients: Types: mobile phones, PDAs, laptop computers, vehicle-mounted devices, hybrid devices Device limitations: considerations for user interface and application design Device location technology: GPS, triangulation Mobile client software, Mobile device operating systems, Micro browsers Mobile device communications protocols: WAP, i-Mode, Mobile device page description languages, Mobile device application software</p>	06
3	<p>Mobile Commerce: Theory And Applications: The Ecology Of Mobile Commerce, The Wireless Application Protocol, Mobile Business Services, Mobile Portal, Factors Influencing The Adoption Of Mobile Gaming Services, Mobile Data Technologies And Small Business Adoption And Diffusion, E–Commerce In The Automotive Industry, Location–Based Services: Criteria For Adoption And Solution Deployment, The Role Of Mobile Advertising In Building A Brand, Mobile financial services, Mobile proactive service management, Mobile auction, Mobile entertainment, Mobile distance education, Mobile information access, Vehicular mobile commerce, Telematics</p>	06
4	<p>Management of mobile commerce services : Content development and distribution to hand-held devices, content caching, pricing of mobile commerce services The emerging issues in mobile commerce : The role of emerging wireless LANs and 3G/4G wireless networks, personalized content management, implementation challenges in m-commerce, futuristic m-commerce services</p>	04
5	<p>M-commerce trust, security, and payment: Trust in m-commerce, Encryption, Authentication, confidentiality, integrity, and non-repudiation, Mobile payment M-commerce issues: Technology issues, Mobile client issues, Communications infrastructure issues, Other technology issues, Application issues, Global m-commerce issues Security Issues: Introduction, Information security, Security techniques and Algorithms, security Protocols, Public Key Infrastructure, Trust, Security Models, Security Frameworks for Mobile Environment</p>	10

6	Business–To–Business Mobile E– Commerce: Enterprise Enablement, Email And Messaging, Field Force Automation (Insurance, Real Estate, Maintenance, Healthcare), Field Sales Support (Content Access, Inventory), Asset Tracking And Maintenance/Management, Remote IT Support, Customer Retention (B2c Services, Financial, Special Deals), Warehouse Automation, Security.	08
---	--	----

Text Books :

1. Mobile Commerce: Technology, Theory and Applications by Brian Mennecke and Troy J. Strader, Idea Group Publishing

Reference Books:

1. Mobile Commerce and Applications, Upkar Varshney, A tutorial at IEEE International Conference on Wireless Communications (WCNC)
2. Mobile Commerce: Frameworks, Applications and Networking Support, ACM/Kluwer Journal on Mobile Networks and Applications (MONET), June 2002 (Upkar Varshney and Ron Vetter)
3. Location-based Mobile Commerce Services, ACM Transactions on Internet Technology, August 2003, (Upkar Varshney)
4. Mobile Commerce: An Emerging Frontier, IEEE Computer, Oct 2000 (Varshney and others)
5. Ravi Kalakota, B.Andrew Whinston, “Frontiers of Electronic Commerce”, Pearson Education, 2003.
6. P. J. Louis, “M-Commerce Crash Course”, McGraw- Hill Companies February 2001.
7. Paul May, “Mobile Commerce: Opportunities, Applications, and Technologies Of Wireless Business” Cambridge University Press March 2001.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW1023	Global Cyber Warfare	04
Module	Detailed content	Hours
1	Cyberspace as a Warfare Domain : Purpose, Plausibility, and Limits of Cyberwar ,Netcentricity ,Operational Cyberwar , A Conceptual Framework , Act of War, Relationship to IO	04
2	Operational History of Cyber Warfare: Cyber Crime , Future Threats , Rise of Nonstate Hacker, Noteworthy Events, Ex. Gaza Cyber war	02
3	Responding to International Cyber Attacks : Law of War, Nonstate actors and Law of War ,Analysing Cyber Attacks , Technological Limitations , Issues , Intelligence Component of Cyber Warfare ,Korean DDOS Attacks,One year after RU-GE War ,Ingushetia Conflict , Predictive Role of Intelligence ,Nonstate Hackers and Social Web ,Dark side of Social Networks, TwitterGate , Automating Process, False Identities,Components of Bulletproof Networks,SORM-2, Kremlin and Russian Internet.	06
4	Organized Crime in Cyber space : Subtle Threat ,Atrivo/Interchange,EST Domains,McColo, Russian Organized Crime and Kremlin Investigating Attribution : Using Open Source Internet Data , Autonomous System Network , Team Cymru and It's Darknet Report, Using WHOIS	04
5	Weaponizing Malware: New Threat Landscape, StopGeogia.ru Malware Discussions , Twitter as DDoS Command Post against Iran , Social Engineering , Channel Consolidation, Adversary's Look at LinkedIn, BIOS Based Rootkit Attack , Malware for Hire , Targeted Attacks Against Military Brass and Government Executives.	04
6	Role of Cyber in Military Doctrine: Russian Federation, FEP ,Information wars, RF Military Policy, Art of Misdirection China Military Doctrine ,Anti-access Strategies , 36 Stratagems , US Military Doctrine	04
7	Advice for Policymakers : Shoot the Hostage, Use Active Defences to Defend Critical Information Systems, Scenarios and Options to Responding to Cyber Attacks, Nation Cyber Security. Conducting Operation : Anarchist Clusters, Social Networks, Social Media, Globalization.	04
8	Russian Federation : Information Warfare Framework Russian Government Policy, Laws and Amendments, Government Structures, Russian Military of Defence ,Administrative Changes, Electronic Warfare Troops , Military Units , Russian Federation Ministry of Communications and Mass Communications US Department of Defence Cyber Command and Organizational Structure	06

9	Active Defence for Cyber : Covert Action , Cyber Active Defence Under International Law ,Cyber Active Defences as Cover Action Under International Law,Cyber Attacks Under International Law : Nonstate Actors	04
---	--	----

Reference Books:

- 1 Inside Cyber Warfare: Mapping the Cyber Underworld by Jeffrey Carr, 2nd edition, O,Reilly
- 2 Cyberdeterrence and Cyberwar by Martin C. Libicki

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW101L	Laboratory 1	04

Module	Detailed content	Hours
1	Laboratory Practicals to be conducted for the subject Computer Network and Design (ICW101)	24

Modality and Assessment:

1. Each Laboratory assignment will be done in a group of two students. The Faculty teaching each core subject will be required to propose and evaluate the respective Laboratory assignments. These will be essentially hands-on practical and not theory / research review types of assignments.
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ICW102L	Laboratory II	04

Module	Detailed content	Hours
1	Laboratory Practicals to be conducted for the subject Web Application Hacking –I. (ICW103)	24

Modality and Assessment:

1. Each Laboratory assignment will be done in a group of two students. The Faculty teaching each core subject will be required to propose and evaluate the respective Laboratory assignments. These will be essentially hands-on practical and not theory / research review types of assignments.
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ICW201	Network Security	04

Module	Detailed content	Hours
1	Security Problem in TCP/IP Protocol Suite: Identification of Security issues in Ethernet, ARP, IP, TCP, Application and Routing protocols.	02
2	Security Models: Military and civil security, vulnerability and threat models, End-end security (COMSEC), link encryption (TRANSEC), compartments. Privacy. Authentication. Denial of service. Nonrepudiation. Issues in multi-level secure systems. Internet security models: IPv4/IPv6 encapsulation header	04
3	Security at Network Layer Routing algorithm vulnerabilities: route and sequence number spoofing, instability and resonance effects. Information hiding: DMZ networks, route aggregation and segregation ICMP redirect hazard: denial of service. ARP hazard: phantom sources, ARP explosions and slow links. Defending against Chernobyl packets and meltdown. Fragmentation vulnerabilities and remedies: (ICMP Echo overrun) IPSec: IP Security Overview, IP Security Architecture, Security Associations, Security Association Database, Security Policy Database, Tunnel and Transport mode, AH and ESP, IP and IPv6, Encapsulating Security Payload, Internet Key Exchange	08

4	Security at Transport Layer: SSL and TLS Secure network infrastructure services: DNS, NTP, SNMP, SSL Architecture, SSL/TLS Basic Protocol, SSL Message Formats, Session Resumption, Computing the keys, Client Authentication, PKI as deployed by SSL, Version Numbers, Negotiating Cipher Suites, Negotiating Compression Methods, Exportability, Encoding, Mobile systems: Address Export and re-use. Session key management: Blind-key cryptosystems (NTP).	06
5	Security at Application Layer: PGP, S/MIME E-mail security, PGP, PEM, S/MIME, Secure binding of multimedia streams, Secure RTP. Secure RSVP.	04
6	Firewalls and IDS Firewalls: Network partitioning, firewall platforms, partitioning models and methods, Secure SNMP, Secure routing interoperability: virtual networks (DARTnet/CAIRN). Transparent and opaque network services. Source masking and hidden channels. IDS, Honeypots, Honey nets,	04
7	Wireless Network Security: Introduction, How wifi works, WEP, Technique of hacking wireless network, countermeasure	04
8	Network Packet analysis: Packet analysis and Packet sniffing in Hub and Switched environment, Analysis of packet for security i.e Sync Scan, OS Fingerprinting	04
9	NOS Security issues: Windows and Linux environment	04

Text Books:

1. Stallings, W., "Cryptography and Network Security: Theory and Practice", Second Edition, John Wiley
2. "Charles P. Pfleeger "Security in computing", Pearson Education

Reference Books :

1. Stalling W., "Network Security Essentials", Pearson
2. Garfinkel S., Spafford G., "Practical Unix and Internet Security", O'Reilly
3. Blacharski D., "Network Security in a Mixed Environment"
4. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by Chris Sanders

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four

questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW202	Cyber Law	04

Module	Detailed content	Hours
1	Introduction: Laws, Investigation and Ethics: Cyber Crime, Information Security and Law, Types & overview of Cyber Crimes, Cyber Law Issues in E-Business Management Overview of Indian IT Act, Ethical Issues in Intellectual property rights, Copy Right, Patents, Data privacy and protection, Domain Name, Software piracy, Plagiarism, Issues in ethical hacking.	08
2	Fundamentals of IT Security Law and Policy: Security Policy, Privacy Notice & Privacy Laws, Computer Crime Laws, Intellectual Property, Non-Disclosure Agreements and Terms of Use, Honeypots & Entrapment, Active Defenses, Hacking Back	06
3	E-Records, E-Discovery and Business Law: Vicarious Liability, E-Discovery, Records Retention, Destruction, Email Retention, Forensics, Privacy Policies, Evidence Law, Signatures	04
4	Contracting for Data Security and Other Technology: Click Through Agreements, Contract Formation, Battle of the Forms, Liability, Breach, Bonds, Assent, Warranty, Remedies, Liens, Ownership Issues, Subpoenas, Documentation, Audits, Exceptions, Maintenance, Termination, Escrow, Investigations, Competition, Disputes, Non-Disclosure	06
5	The Law of IT Compliance: How to conduct investigations: Cooperation with investigations, Numerous Examples of Fraud (Post-Mordems), SOX, Securities Fraud, Federal Sentencing Guidelines, Codes of Ethics, Hotlines, Reporting, Whistleblowing, Employee Monitoring, Entrapment, Raids & Seizures	06
6	Applying Law to Emerging Dangers: Cyber Defense Sony Root Kit Case Study, Crisis Communications, Choicepoint Case Study, Relationship with Law Enforcement, TJX Case Study, Publicity, Safely Monitoring Threats w/o Incurring Liability, Factors Mitigating Legal Risk, Public Accountability, Political Diplomacy, Strategic Legal Procedures, Competitive Boundaries	08

Text Book:

1. Sood, "Cyber Laws Simplified", Mc Graw Hill

Reference Books:

1. Anthony Reyes, "Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors"
2. Marcia P. Miceli, "Whistle-Blowing in Organizations",

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW102	Cryptography and PKI	04
Module	Detailed content	Hours
1	Cryptography: Concepts and Techniques: Introduction, Security Trends, Model for Network Security, Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Steganography, Key Range and Key Size, Possible Types of Attacks	08
2	Symmetric Key Algorithms: DES, 3DES, AES, IDEA, RC4, RC5, Confidentiality using symmetric encryption.	04
3	Introduction to Number Theory: Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms Public- Key Cryptography and RSA: Principles of Public-Key Cryptosystems, RSA, Key Management, Diffie-Helman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.	08
4	Message Authentication and Hash Functions: Authentication Requirements, Authentication Functions, MAC, Hash Functions, Security of Hash Functions and MACs, SHA, HMAC	04
5	Digital Signatures and Public Key Infrastructure (PKI): Digital Signatures, Authentication Protocols, DSS, Authentication Applications: Kerberos, X.509 Authentication Service Digital Certificates, Private Key Management, PKI Trust Models, Public Key Cryptography Standards, Revocation, Directories and PKI, PKIX and Security.	08
6	Elliptic Curves: The Addition Law, Elliptic curve Mod p, Factoring with Elliptic Curves, Elliptic Curve Cryptosystems	02
7	Cryptography in Java, .NET and Operating Systems: Cryptographic Solutions using Java, Cryptographic Solutions using Microsoft .NET Framework, Cryptographic Toolkits, Security and Operating Systems, Database Security.	06

Text Books:

1. Information Security Principal and Practice: Mark stamp, Wiley
2. Cryptography and security, wiley,Shyamala,harini

Reference Books:

1. Stallings, W., "Cryptography and Network Security", Fourth Edition, Pearson
2. Introduction to Cryptography with coding Theory, Pearson,WadenTrappe
3. Forouzan B., "Cryptography and Network Security", Second Edition, Tata McGraw Hill

4. Bernard Menezes, "Network Security and Cryptography", Cengage Learning.
5. Charlie Kaufman, Radia Perlman and Mike Speciner "Network security, private communication in a public world" , Second Edition, Pearson

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW2011	Information security and risk management	04

Module	Detailed content	Hours
1	Introduction to assessing Network Vulnerabilities: type and procedure of network vulnerability assessment	04
2	Principles of Security: Information Classification, Policy framework, role based security in an organization	06
3	Risk Assessment: Laws, Mandates and Regulations, Risk assessment best practices, Risk assessment best practice.	06
4	Risk Assessment Methodologies: Defence –in depth approach, risk analysis, Asset valuation approach, Quantitative and Qualitative risk- assessment approaches. Scoping the project, Understanding the attacker.	08
5	Performing the Assessment: Vulnerability scan and Exploitation: Internet Host and network enumeration, IP network Scanning, Assessing Remote Information Services, Assessing Web servers, Assessing Web Applications, Assessing Remote Maintenance Services, Assessing Database services, Assessing Windows Networking Services, Assessing Email services.	08
6	Open source tools used for Assessment and Evaluation, and exploitation framework	04
7	Final Report Preparation and Post Assessment Activists	04

Text books:

1. Network Security assessment, Chris McNab, O'reilly
2. Inside Network Security Assessment, Michael Gregg, Pearson

Reference Books :

1. Security in Computing, fourth Edition, Charles Pfleeger, Pearson
2. The Security Risk Assessment Handbook: Douglas LanDoll, Auerbach Publication.
3. Nina Godbole, "Information Systems Security", Wiley
4. Cyber Security: Sunit Belapur, Wiley
5. Whitman & Mattord. Management of Information Security. Thomson Course Technology (2004). ISBN: 0-619-21515-1

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW2012	Social Engineering and Reality Mining	04

Module	Detailed content	Hours
1	Social Network- Networks and relation, Analysis of network data, interpretation of network data, pervasive computing.	06
2	Social network Analysis- Metrics in Social network analysis, social network analysis tools and libraries, Network intelligence- Managing network intelligence	06
3	Mathematical Representation of social networks- Graphs and matrices, Sociometric analysis, Poisson Random network, Exponential Random graph models, Fuzzy models applied to complex social system analysis	06
4	Handling Social Data- Organization of relational data, storage of relational data, selection of relational data.	04
5	Reality Mining- Concept, Tradeoffs in traditional social data gathering, new instruments for behavioural data collection, inferring social network structure using mobile phone data, Predicting behavior of technosocial systems, Big data, applications, challenges	06
6	Complex Social Systems- Complex networks, clustering degree distribution, social proximity sensing reality mining as proximity sensing technology, mobile social software, privacy implications. Case study- Extracting influential nodes on a social network	06
7	Social Engineering- Pretexting, diversion theft, phishing, quid pro quo, tailgating. Reverse social engineering attacks in online social networks.	06

Text Books :

1. John Scott, "Social Network Analysis- a Handbook", II edition, Sage Publication
2. Stanley Wasserman, Katherine Faust, "Social Network Analysis- Methods and Applications", Cambridge University Press

Reference:

1. Ph.D. Thesis of Alex (Sandy) Pentland, Massachusetts Institute of Technology (MIT) USA.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination

Subject Code	Subject Name	Credits
ICW203	Web Application Hacking II	04
Module	Detailed content	Hours
1	Attacking Users: Cross-Site Scripting (XSS) Varieties of XSS, XSS Attacks in Action, Finding and Exploiting XSS Vulnerabilities, Preventing XSS Attacks.	04
2	Attacking Users: Other Techniques Inducing User Actions, Capturing Data Cross-Domain, Client-Side Injection Attacks, Local Privacy Attacks, Attacking ActiveX Controls, Attacking Browser	06
3	Automating Customized Attacks Uses for Customized Automation, Enumerating Valid Identifiers, Harvesting Useful Data, Fuzzing for Common Vulnerabilities, Burp Intruder, Barriers to Automation	06
4	Exploiting Information Disclosure and vulnerabilities Exploiting Error Messages, Using Inference, Preventing Information Leakage, Buffer Overflow Vulnerabilities, Integer Vulnerabilities, Format String Vulnerabilities	04
5	Attacking Application Architecture and Server Tiered Architectures, Shared Hosting and Application Service Providers, Vulnerable Server Configuration, Vulnerable Server Software, Web Application Firewalls	06
6	Finding Vulnerabilities in Source Code Approaches to Code Review, Signatures of Common Vulnerabilities, Java Platform, ASP.NET, PHP, Perl, Database Code Components, Tools for Code Browsing	04
7	Web Application Hacker's Toolkit Web Browsers, Integrated Testing Suites, Standalone Vulnerability Scanners, Other Tools	04
8	A Web Application Hacker's Methodology Map Application's Content, Analyze Application, Test Client-Side Controls, Test Authentication Mechanism, Test Session Management Mechanism, Test Access Controls, Test for Input-Based Vulnerabilities Test for Function-Specific Input Vulnerabilities, Test for Logic Flaws, Test for Shared Hosting Vulnerabilities, Test for Application Server Vulnerabilities	06

Text Book :

1. Web Application Hacker's Handbook, Dafydd Stuttarf , Marcus Pinto, Wiley

Reference Books :

1. Hacking Exposed Web Applications, 3rd Edition, by Joel Scambray, Vincent Liu and Caleb Sima.

2. Web Application Defender's Cookbook: Battling Hackers and Protecting Users by Ryan C. Barnett and Jeremiah Grossman

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW2021	Storage Area Networks	04

Module	Detailed content	Hours
1	Concepts of storage networks: Data Storage and Data Access Problem, the battle of size and access, decoupling the storage component: putting storage on the network, creating network for storage.	04
2	Storage area network : Introduction to SAN, Components of SAN, fibre channels ,FC connectivity, ports, FC architecture ,zoning, FC login types, topologies	04
3	Network Attached Storage: Benefits, NAS file I/O , Components, Implementations, Sharing Protocols, AS I/O operations , Factors affecting NAS Performance and Availability, IP SAN: Iscsi, fcip	06
4	Content-addressed storage: Fixed Content and Archives, Types of Archives, Features and Benefits of CAS,CAS Architecture, Example	02
5	Storage virtualization: Forms of Virtualization, Storage Virtualization Configuration and Challenges, Types of Storage Virtualization.	02
6	Basic software for storage networking : Software For SANs, Shared access data Managers, Volumes: Resilience, performance, and Flexibility, File Systems and Application performance	03
7	Killer Applications for SAN: Backup, Highly available data, Disaster Recoverability, Clusters, Data Replication.	05
8	Enterprise backup software for SAN: Backup Management, Enterprise data Protection, Backup architecture, Backup policies, Minimizing impact of Backup	04
9	SAN management and Security: Managing SANs, SAN management, Basics, Ideal Environment, Quality of Online Storage Service, Backup Cost Backup Impact, Allocation	06
10	Securing storage infrastructure: Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking	04

Text Books :

- 1 Richard Barker, Paul Massiglia, “Storage Area Network Essentials: A Complete Guide to Understanding and Implementing SANs”, Wiley India

2 G. Somasundaram, Alok Shrivastava, "Information Storage and Management", EMC Education services", Wiley Publication

Reference Books :

1 Ulf Troppen, Rainer Erkens, Wolfgang Muller, "Storage Networks Explained", Wiley publication

2 Robert R. Korfhage, "Information Storage and Retrieval", Wiley Publication

3 John R. Vacca, Michael Erbschloe, "The Essential Guide to Storage Area Networks," Prentice Hall.

4 Tom Clark, "IP SANS: An Introduction to iSCSI, iFCP, and FCIP Protocols for Storage Area Networks," Addison-Wesley.

5 Alan F. Benner, "Fibre Channel for SANs," McGraw-Hill.

6 Ralph H. Thornburgh, Barry J. Schoenborn, "Storage Area Networks: Designing and Implementing a Mass Storage System," Prentice Hall.

7 Marc Farley, "Building Storage Networks," McGraw-Hill.

8 Thomas Clark, "Designing Storage Area Networks," Addison-Wesley.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination

Subject Code	Subject Name	Credits
ICW2022	Intrusion Detection Systems	04

Module	Detailed content	Hours
1	Intrusion Detection Systems : IDS Introduction, Types of IDS : Host IDS, Network IDS, Target Based Assembly Detection, Signature and Anomaly Based Detection , Signature Writing Techniques.	06
2	Lifecycle of Vulnerability : Packet Analysis and Signature Writing, Signature Tuning , Advanced Examples	04
3	Proactive Intrusion Prevention and Response via Attack Graphs : Topological Vulnerability Analysis, Attack Modeling and Simulation , Optimal Network Protection , Intrusion Detection and Response	06
4	Network Flows and Anomaly Detection : IP Data Flows , IPFIX Protocol , Behavioural Analysis and anomaly Detection , Differentiation Between IDS and Netflow	04
5	Traffic Analysis: Packet Dissection Using TCPdump, Dissecting the Whole Packet, Freeware Tools for Packet Dissection, Examining IP Header Fields, Introduction to Snort and Rules.	06
6	Wireless IDS/IPS : Types , Wireless IDS Events, Intrusion Prevention Techniques , Honeypot, Other Wireless Threats.	04
7	Physical and Geospatial Intrusion Detection for IT : Common Physical Access Control Components , Geographic Information System , Spatial Point Pattern Analysis , Point Intensity , Geocoding Techniques , Limitations.	06
8	Visual Data Communications : Visualization , Statistical Graphing Techniques , Technological Considerations , Security Event Visualization	04

Text Book:

- 1 .Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century, Ryan Trost, Addison-Wesley Professional; 1 edition

Reference books

1.Rebecca Gurley Base “ Intrusion Detection” MacMillan Technology Series(MTP Series) ISBN
1578701856, 9781578701858

2. Rafeeq Rehman “ Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID” Prentice Hall
PTR ,2003 ISBN 0-13-140733-3

3.Network Intrusion Detection, Third Edition : By Stephen Northcutt, Judy Novak.

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination

Subject Code	Subject Name	Credits
ICW2023	Advanced Computer Forensic Analysis	04

Module	Detailed content	Hours
1	Overview of computer Forensics Technology- Introduction to computer forensics, use of forensics in law enforcement, employment proceedings, computer Forensics services. Types of computer Forensics Technology- Military, law, spyware and Adware, Biometrics security systems.	06
2	Types of Computer Forensics systems Internet security, IDS, Firewall, Public key, net privacy systems, vendor and computer Forensics services.	06
3	Computer Forensics evidence and capture Data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, computer image verification and authentication	06
4	Computer Forensics Analysis Discovery of electronic evidence- electronic document discovery, identification of data- Time keeping, forensic identification and analysis of technical surveillance devices. Reconstructing fast events	08
5	The information warfare Arsenal and Tactics of terrorists and Rogues The Terrorist profile, the dark world of the cyber underground, new tools of terrorism, information warfare, Arsenal and Tactics of private companies.	08
6	Civilian casualties The violation of privacy during information wars. The individual exposed. Advanced computer Forensics systems and future directions- advanced encryption, hacking, advanced trackers, case studies.	06

Text Books:

1. Cyber Security : Belapure: wiley
2. By John R. Vacca Computer forensics: computer crime scene investigation, Volume 1

Reference Books :

1. EnCase Computer Forensics . Sybex
2. Computer Forensics: Incident Response Essentials, Warren G. Kruse II & Jay G. Heiser
3. Computer Forensics & Privacy, Michael Caloyannides
4. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, edited by Albert J. Marcella Jr. & Robert S. Greenfield
5. Handbook of Computer Crime Investigation, edited by Eoghan Casey

Assessment:

Internal:

Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:

Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ICW203L	Laboratory III	04

Module	Detailed content	Hours
1	Laboratory Practicals to be conducted for the subject Network Security (ICW201).	24

Modality and Assessment:

1. Each Laboratory assignment will be done in a group of two students. The Faculty teaching each core subject will be required to propose and evaluate the respective Laboratory assignments. These will be essentially hands-on practical and not theory / research review types of assignments.
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ICW204L	Laboratory IV	04

Module	Detailed content	Hours
1	Laboratory Practicals to be conducted for the subject Cryptography and PKI (ICW203)..	24

Modality and Assessment:

1. Each Laboratory assignment will be done in a group of two students. The Faculty teaching each core subject will be required to propose and evaluate the respective Laboratory assignments. These will be essentially hands-on practical and not theory / research review types of assignments.
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ICWS301	Seminar	03

Guidelines for Seminar

- o Seminar should be based on thrust areas in Information and Cyber Warfare.
- o Students should do literature survey and identify the topic of seminar and finalize in consultation with Guide/Supervisor. Students should use multiple literatures (at least 10 papers from Refereed Journals) and understand the topic and compile the report in standard format and present in front of Panel of Examiners. (pair of Internal and External examiners appointed by the University of Mumbai)
- o **Seminar should be assessed based on following points**
 - Quality of Literature survey and Novelty in the topic
 - Relevance to the specialization
 - Understanding of the topic
 - Quality of Written and Oral Presentation

IMPORTANT NOTE:

1. Assessment of Seminar will be carried out by a pair of Internal and External examiner. The external examiner should be selected from approved panel of examiners for Seminar by University of Mumbai, OR faculty from Premier Educational Institutions /Research Organizations such as IIT, NIT, BARC, TIFR, DRDO, etc. OR a person having minimum Post-Graduate qualification with at least Ten years' experience in Industries.
2. Literature survey in case of seminar is based on the broader area of interest in recent developments and for dissertation it should be focused mainly on identified problem.
3. At least 4-5 hours of course on Research Methodology should be conducted which includes Literature Survey, Problems Identification, Analysis and Interpretation of Results and Technical Paper Writing in the beginning of 3rd Semester.

Subject Code	Subject Name	Credits
ICWD301 / ICWD401	Dissertation I & II	12 + 15

Guidelines for Dissertation

o Students should do literature survey and identify the problem for Dissertation and finalize in consultation with Guide/Supervisor. Students should use multiple literatures and understand the problem. Students should attempt solution to the problem by analytical/simulation/experimental methods. The solution to be validated with proper justification and compile the report in standard format.

Guidelines for Assessment of Dissertation I

o Dissertation I should be assessed based on following points

- Quality of Literature survey and Novelty in the problem
- Clarity of Problem definition and Feasibility of problem solution
- Relevance to the specialization
- Clarity of objective and scope
- Dissertation I should be assessed through a presentation by a panel of Internal examiners appointed by the Head of the Department/Institute of respective Programme.

Guidelines for Assessment of Dissertation II

o Dissertation II should be assessed based on following points

- Quality of Literature survey and Novelty in the problem
- Clarity of Problem definition and Feasibility of problem solution
- Relevance to the specialization or current Research / Industrial trends
- Clarity of objective and scope

- Quality of work attempted
 - Validation of results
 - Quality of Written and Oral Presentation
- o Dissertation II should be assessed through a presentation jointly by Internal and External Examiners appointed by the University of Mumbai
- o Students should publish at least one paper based on the work in reputed International / National Conference (desirably in Referred Journal)