# Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)
## Scheme of Teaching & Examination
### M. Tech. (e-Security)
#### Department: INFORMATION TECHNOLOGY

**2nd Semester**

<table>
<thead>
<tr>
<th>S. No</th>
<th>Board of Study</th>
<th>Subject Code</th>
<th>Subject</th>
<th>Periods per Week</th>
<th>Scheme of Examination</th>
<th>Total Marks</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
<td>P</td>
<td>ESE</td>
</tr>
<tr>
<td>1</td>
<td>Information Technology</td>
<td>577211 (33)</td>
<td>Trusted Internet</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Information Technology</td>
<td>577212 (33)</td>
<td>Business Ethics and Cyber Laws</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>Information Technology</td>
<td>577213 (33)</td>
<td>Advanced Cryptography</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>Information Technology</td>
<td>577214 (33)</td>
<td>Security Threats and Management</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>5</td>
<td>Refer Table - II</td>
<td>Elective - II</td>
<td></td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>6</td>
<td>Information Technology</td>
<td>577221 (33)</td>
<td>Secured Operating System Lab</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td>7</td>
<td>Information Technology</td>
<td>577222 (33)</td>
<td>Image Processing and Security Lab</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15</td>
<td>5</td>
<td>6</td>
<td>650</td>
</tr>
</tbody>
</table>

**Note (1)** Choice of elective once made for an examination cannot be changed in future examinations.

**Note (2)** Examination Duration of all Theory papers will be of THREE hours.
UNIT I
**Internet:** Understanding the Internet, Hardware Requirements to connect to the internet, Software requirements and Internet Service Providers (ISP), Internet Addressing, Internet Protocol: Routing Information Protocol (RIP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Domain Name Service (DNS), Basic Connectivity: Telnet, FTP, Internet Relay Chat (IRC).

UNIT II
**Access Attacks:** Hacker Techniques – Snooping, Eavesdropping, interception, Hacker’s motivation, Historical Hacking Techniques; Advance Techniques, Targeted Hacker, Information Security Services – Confidentiality, Integrity, Availability and Accountability.

UNIT III
**Firewalls:** Concepts, Types of Firewalls, Firewall Configuration, Design a Firewall Rule set, Purpose of Firewall, Security role of a Firewall, Advantages and disadvantages of firewall, Firewall Components, Procuring a Firewall, Administrating a firewall, firewall toolkits.

UNIT IV
**Encryption:** Basic Concepts, Private Key Encryption, Public Key Encryption, Digital Signature, Trust in the System, Encryption Algorithm – RSA Encryption, Blowfish Encryption.

UNIT V
**Security Mechanism:** User Authentication, Attacks from inside the system, Attacks from outside the system, Protection Mechanism: Snooping, Eavesdropping, interception, Trusted Systems, Trusted Computing Base, Formal Models of Secure system, Multi-level security, designing trusted Operating System.

TEXT BOOKS:

REFERENCES:
Semester: **M.TECH. IIInd**  
Specialization: **e-Security**  
Subject: **Business Ethics and Cyber Laws**  
Code: 57212 (33)  
Total Theory Periods: **40**  
Total Tutorial Periods: **12**  
Minimum number of class test to be conducted: **02**

**UNIT – I**  
**Business Ethics:** Principles of Business Ethics- Ethical philosophies, Ethical management. Corporate Governance - principles, mechanisms and control. Corporate Social Responsibility – approaches, social accounting, auditing and reporting, Benefits of Corporate Social Responsibility.

**UNIT – II**  
**Ethical Practices:** Creating an ethical organization. Workplace Ethics, Environment and Ethics, Ethics in Marketing and Consumer Protection, Ethics in Accounting and Finance, Ethics in Human Resource Management, intellectual property and skills.

**Unit III**  
**Cyber Crimes:** Related concepts, distinction between cyber crimes and conventional crimes, Cyber criminals and their objectives, Kinds of cyber crimes cyber-stalking, cyber pornography, forgery and fraud, crime related to IPRs, cyber terrorism, computer vandalism etc. Cyber forensics, digital forensics and the law, forensic evidence, digital forensic tools.

**Unit IV**  
**Legal Issues in Cyber Crime:** Issues relating to investigation, issues relating to jurisdiction, issues relating to evidence, relevant provisions under Information Technology Act 2000, Indian penal code, Pornography Act and Indian Evidence Act.

**Unit V**  
**Copyright Issues:** Linking, framing, protection of content on web site, international treaties, trade mark issues in cyberspace, domain name dispute, cyber squatting, uniform dispute resolution policy, computer software and related IPR (Intellectual Property Rights) issues.

**TEXT BOOKS:**

4. M C Kuchhal, Business Law, Vikas publishing, New Delhi

**REFERENCES:**

UNIT I
OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.

UNIT II
Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption, Public key cryptography and RSA.

UNIT III
Authentication requirements: Authentication functions, Message authentication codes, Hash functions, Security of hash functions and MACs, MD5 Message Digest algorithm, Secure hash algorithm, Ripend, HMAC digital signatures, Authentication protocols

UNIT IV
Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell’s theorem, Bell basis, teleportation of a single qubit – theory and experiments.

UNIT V
Future trends: Review of recent experimental achievements, study on technological feasibility of a quantum computer, candidate physical systems and limitations imposed by noise.

TEXT BOOKS:


REFERENCES:

UNIT I
Introduction: Security threats, Sources of security threats, Motives , Target Assets and vulnerabilities, Consequences of threats, E-mail threats, Web-threats, Intruders and Hackers, Cyber crimes.

UNIT II

UNIT III

UNIT IV

UNIT V

TEXT BOOKS:

REFERENCES:
UNIT I

UNIT II

UNIT III

UNIT IV
Implementation Issues: WLAN Configuration, IEEE 802.11, Physical layer, media access frame format, systematic exploitation of 802.11b, WLAN, WEP – WEP Decryption script, overview of WEP attack, Implementation, Analyses of WEP attacks.

UNIT V

TEXT BOOKS:

REFERENCES:
UNIT - I

UNIT - II
Desktop Grids: Background, Definition, Challenges, Technology, Suitability, Grid server and practical uses, Clusters and Cluster Grids, HPC Grids, Scientific in sight, Application and Architecture, HPC application, Development Environment and HPC Grids, Data Grids, Alternatives to Data Grid, Data Grid architecture.

UNIT - III
Architecture and Services: The open Grid services Architecture, Analogy, Evolution, Overview, Building on the OGSA platform, Implementing OGSA based Grids, Creating and Managing services, Services and the Grid, Service Discovery, Tools and Toolkits, Universal Description Discovery and Integration (UDDI).

UNIT - IV

UNIT - V
Emerging Areas: Application integration, Application classification, Grid requirements, Integrating applications with Middleware platforms, Grid enabling Network services, Managing Grid environments, Managing Grids, Management reporting, Monitoring, Data catalogs and replica management, Portals, Different application areas of Grid computing.

TEXT BOOKS:

REFERENCES:
UNIT I

UNIT II
Survey of Steganographic techniques: Substitution system and bitplane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

UNIT III
Steganalysis: Detecting hidden information: text, audio, video and images, Extracting hidden information, Disabling hidden information, Watermarking techniques, Basic Message Coding, Error Correction coding, Information Theoretic analysis and design issues, Evaluation and benchmarking of watermarking system.

UNIT IV
Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace: binary image, audio, video. Formatting the watermark beds - Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions.

UNIT V
Data Right Management: DRM Products and Laws, Fingerprints – Examples, Protocols and Codes – Boneh-Shaw finger printing Scheme, Steganography and watermarking applications – Military, Digital copyright protection and protection of intellectual property.

TEXT BOOKS:


REFERENCES:

List of Experiments:

(Implement the following on LINUX platform. Use C for high level language implementation)
1. Shell programming
   - command syntax
   - write simple functions
   - basic tests
2. Shell programming
   - loops
   - patterns
   - expansions
   - substitutions
3. Write programs using the following system calls of UNIX operating system:
   fork, exec, getpid, exit, wait, close, stat, opendir, readdir
4. Write programs using the I/O system calls of UNIX operating system (open, read, write, etc)
5. Write C programs to simulate UNIX commands like ls, grep, etc.
6. Given the list of processes, their CPU burst times and arrival times, display/print the Gantt chart for CPU burst times for FCFS and SJF. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
7. Given the list of processes, their CPU burst times and arrival times, display/print the Gantt chart for Priority and Round robin. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
8. Implement the Producer – Consumer problem using semaphores.
9. Write a shell script to scan current operating system security settings.
10. Write a program to create a secured pipe for Inter-Process Communication.
11. Identify Vulnerabilities (Potential Threats) of Operating System and Security features.
12. Identify and analyze Buffer overflow problem.
13. Implement some memory management schemes – I for e.g.
   Free space is maintained as a linked list of nodes with each node having the starting byte address and the ending byte address of a free block. Each memory request consists of the process-id and the amount of storage space required in bytes. Allocated memory space is again maintained as a linked list of nodes with each node having the process-id, starting byte address and the ending byte address of the allocated space.
14. Implement some memory management schemes – II for e.g.
   When a process finishes (taken as input) the appropriate node from the allocated list should be deleted and this free disk space should be added to the free space list. Care should be taken to merge contiguous free blocks into one single block. This results in deleting more than one node from the free space list and changing the start and end address in the appropriate node. For allocation use first fit, worst fit and best fit.
List of Experiments:

1. Study and Analyze important Image Processing toolbox functions with at least two standard images like Cameraman, Lena, Monkey, and others.
2. Write a program for Image reading and displaying the results in matrix form and hence changing the matrix elements by multiplying with the factor 0.001 and hence writing to a file with extension .jpeg format and hence plot a histogram.
3. Write a program for performing Point-to-point transformation.
4. Write a program for performing Morphological operations.(The operations that can be performed are erosion, dilation, opening, closing, open-close, close-open.)
5. Write a program to hide a word in an image file and retrieve it (Stenography).
6. Histogram equalization. This experiment illustrates the relationship among the intensities (gray levels) of an image and its histogram. It shows how to improve the image by equalizing the histogram.
7. Write a program for performing Geometric transformations by using translation, rotation scaling of given image.
8. Write a program for performing Linear filtering using convolution. After completing this experiment every student should understand the concepts of filtering using linear convolution.
9. Write a program for applying highly selective filters upon input images. In this experiment students appreciate the effects on an image after a highly selective filter is applied to it.
10. Write a program for performing Non Linear filtering upon input images using convolution masks. This experiment allows students to understand the effects of a median filter on an image corrupted with impulsive noise.
11. Write a program to use Entropy as a compression measure upon input images. This experiment introduces students to entropy as compression measurement to the DPCM compression measure.
12. Write a program for performing Edge detection upon input images. This experiment enables students to understand the concept of edge detectors and their operation in noisy images.
13. Write a program for Converting Color to Gray Scale and hence enhancement with segmentation.