Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Scheme of Teaching & Examination

M.Tech. (Information Security)

UNDER COMPUTER SCIENCE & ENGINEERING BOARD

1st Semester

S.N.	Board of Study	Subject Code	Subject	Periods per Week			Scheme of Examination Theory /Practical			Total Marks	Credit L+(T+P)/2
				L	T	P	ESE	CT	TA		
1	Computer Science & Engg.	571111 (22)	Mathematical Foundations of Information Security	3	1	-	100	20	20	140	4
2	Computer Science & Engg.	571112 (22)	Introduction to Information Security	3	1	-	100	20	20	140	4
3	Computer Science & Engg.	571113 (22)	Operating System Security	3	1	-	100	20	20	140	4
4	Computer Science & Engg.	571114 (22)	Digital Signal and Image Processing	3	1	-	100	20	20	140	4
5	Refer Table – I		Elective – I	3	1	-	100	20	20	140	4
6	Computer Science & Engg.	571121 (22)	Operating System Security Lab	-	-	3	75	-	75	150	2
7	Computer Science & Engg.	571122 (22)	Digital Signal and Image Processing Lab	-	-	3	75	-	75	150	2
Total				**15**	**5**	**6**	**650**	**100**	**250**	**1000**	**24**

L-Lecture, **T**- Tutorial, **P**- Practical, **ESE**- End Semester Examination, **CT**- Class Test, **TA**- Teacher's Assessment

Table – I			
Elective – I			
S.N.	Board of Study	Subject Code	Subject
1	Computer Science & Engg.	571131 (22)	Data Encryption and Compression
2	Computer Science & Engg.	571132 (22)	Information Theory and Coding
3	Computer Science & Engg.	571133 (22)	Wireless Communication

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.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st
Subject: **Mathematical Foundations of Information Security**
Total Theory Periods: **40** hours
Minimum number of Class tests to be conducted: 02

Branch: **Information Security**
Code: **571111(22)**
Total Tutorial Periods: **12 hours**
Total Marks in End Semester Exam: **100**

Unit – I INTRODUCTION TO SET THEORY

Basic concept of set theory, Rough Set theory, Relations, Properties of relation in a set, Equivalence relation, Composition of relations, Partial order & total order relations, Lattices & Hasse diagram, Introduction to function, Inverse, Identity, Injective, Surjective & Bijective functions, Composition of functions and some special functions.

Unit – II INTRODUCTION TO GRAPH THEORY

Introduction to graph theory, Walks, Paths & Circuits, Types of graphs, Shortest path problems, Eulerian and Hamiltonian graphs, Basic concept of tree: Spanning tree, Minimum Spanning tree, Search tree, Rooted Binary tree, Cut sets, Network flow, Matrix representation of graphs.

Unit – III GROUP THEORY & CODING

Basic concept of Group theory, Homomorphism and Isomorphism of groups, COSETS and Lagrange's Theorem, Elements of Coding theory, Group codes, Decoding, Hamming matrices, The Parity check and Generator Matrices.

Unit – IV INTRODUCTION TO NUMBER THEORY

Facts from elementary number theory, Fundamental theorem of arithmetic, G.C.D., Modular Operator, Euclid's algorithm, Modular arithmetic, Fermat's little theorem, Euler's Theorem, Modular Multiplicative Inverse, Primality Testing.

Unit – V INTRODUCTION TO CRYPTOGRAPHY

Introduction to Cryptography, Encryption, Decryption, Integer Factoring Problem, Discrete Logarithm Problem, Hash Function, Digital Signature, Symmetric key Cryptosystem, Public key Cryptosystem, Diffie-Hellman Key Exchange, RSA Cryptosystem, ElGamal Cryptosystem, Elliptic Curve Cryptosystem.

Text Books :
1. J.P. Tremblay and R. Manohar, "Discrete Mathematical Structures with applications to Computer Science", TataMcGraw-Hill, 2000.
2. Swapan Kumar Sarkar, "A Text Book of Discrete Mathematics", S. Chand & Company Ltd., 2001.
3. Gareth A. Jones, Josephine Mary Jones, "Elementary Number Theory", Springer-Verlag, 2004.
4. Neal Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag, 2005.
5. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 2000.
6. Johannes A.Buchman, "Introduction to Cryptography", Springer-Verlag, 2005.

Reference Books :
1. C.L. Liu, "Elements of Discrete Mathematics", Tata McGraw-Hill, 2002.
2. Bernard Kolman, Robert C. Busby, and Sharon Cutler Ross, "Discrete Mathematical Structures", Pearson Education, 2004.
3. Narsingh Deo, "Graph theory with Applications to Engineering and Computer Science", Prentice Hall of India, 2003.
4. J.L. Mott, A. Kandel, and T.P. Baker, "Discrete Mathematics for Computer Scientists and Mathematicians", Prentice Hall of India, 2002.
5. Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols", Ramat Gan, CRC Press Series, 2002.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st

Branch: **Information Security**

Subject: **Introduction to Information Security**
Total Theory Periods: **40 hours**
Minimum number of Class tests to be conducted: 02

Code: **571112 (22)**
Total Tutorial Periods: **12 hours**
Total Marks in End Semester Exam: **100**

Unit – I OVERVIEW OF COMPUTER SECURITY
Essentials of Computer Security, Need for information security, Sources of security threats – Intruders, Viruses, Worms and related threats, Threat identification and Threat analysis - Vulnerability identification and Assessment, Components of Computer Security - Physical Security, System Access & Control, Goals of Information Security.

Unit – II MECHANISMS OF COMPUTER SECURITY SYSTEMS
Cryptography - Public Key Cryptography, Principles of Public Key Cryptosystems, The RSA Algorithm, Key Management – Authentication, Elements, Types and Methods, Digital Signature, Intrusion Detection System (IDS), Types and Challenges, Intrusion Prevention System (IPS) – Firewalls, Design Principles, Scanning, Filtering and Blocking.

Unit - III SOURCES OF ATTACKS AND SECURITY POLICIES
Vulnerabilities – Sources of Vulnerabilities, Cyber Crime and Hackers, Viruses and Content Filtering - Security Assessment, Analysis and Assurance, Computer Network Security Protocol and Standards - Security Policies, Integrity Policies, Confidentiality Policies, Security Models - Access Control Matrix Model, Take-Grant Protection Model.

Unit- IV IP BASED WEB SECURITY AND STANDARDS
Secure Sockets – IPSec Overview, IPSec Architecture, IPSec-Internet Key Exchanging (IKE), IKE phases, Encoding, Internet Security, Threats to privacy – Packet Sniffing, Spoofing, Web Security Requirements – Real Time Communication Security, Security Standards, Kerberos.

Unit -V TRUSTED SYSTEMS USING PROTOCOLS
Security Protocols, Transport Layer Protocols, SSL, Electronic Mail Security, PEM and S/MIME Security Protocol, Pretty Good Privacy, Firewalls Design Principles, Trusted Systems, Electronic Payment Protocols.

Text Books :
1. William Stallings, "Cryptography and Network Security: Principles and Standards", Prentice Hall India, 3rd Edition, 2003.
2. Charlie Kaufman, Radia Perlman, and Mike Speciner, "Network Security: Private Communication in a public world", Prentice Hall India, 2nd Edition, 2002.

Reference Books :
1. Charles P. Pleeger, "Security in Computing", Pearson Education Asia, 2001.
2. William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education Asia, 2000.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st

Branch: **Information Security**

Subject: **Operating System Security**

Code: **571113(22)**

Total Theory Periods: **40**

Total Tutorial Periods: **12**

Minimum number of Class tests to be conducted: 02

Total Marks in End Semester Exam: **100**

Unit-I OVERVIEW OF OPERATING SYSTEMS
Operating System concepts, Process Management and Scheduling, Memory Management: Partitioning, Paging, Segmentation, Virtual memory, Device and File management, Introduction to Operating System Security, Operating System Security Mechanism, Case studies : Linux and Windows.

Unit-II SYNCHRONIZATION AND PROCESSES
Clock Synchronization, Mutual Exclusion, Election Algorithms, Atomic Transactions, Deadlocks, Processes, Threads, System Models, Processor Allocation, Scheduling, Fault Tolerance, Real Time Distributed Systems.

Unit-III SHARED MEMORY AND FILE SYSTEMS
Shared Memory, Consistency Models, Page based distributed shared memory, Shared variables, Object based distributed shared memory, Distributed File Systems: Design and Implementation.

Unit - IV PROTECTION AND SECURITY
Protection and Security - Preliminaries, Operating System Security Models, Vulnerability Analysis and Common Unit Vulnerabilities, Data security, Cryptography: Model of cryptography, Conventional cryptography, Modern cryptography, Private Key Cryptography, Data Encryption Standard, Public Key Cryptography, Multiple Encryption, Authentication in distributed systems.

Unit-V CONCURRENCY CONTROL AND OPTIMIZATION
Database Operating systems : Introduction, Requirements of a database Operating System, Concurrency control : Theoretical Aspects, Introduction, Database Systems, A Concurrency Control Model of database systems, The Problem of Concurrency Control, Serializability theory, Distributed database systems.

Text Books :
1. Andrew S Tanenbaum , " Distributed Operating Systems " , Pearson Education India, 2001.

Reference Books :
1. Mukesh Singhal, Niranjan G Shivratri , "Advanced Concepts in Operating Systems", McGraw Hill International, 1994.
2. Pradeep Kumar Sinha, "Distributed Operating Systems: Concepts and Design", PHI, 2002.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st   Branch: **Information Security**
Subject: **Digital Signal and Image Processing**   Code: **571114 (22)**
Total Theory Periods: **40**   Total Tutorial Periods: **12**
Minimum number of Class tests to be conducted: 02   Total Marks in End Semester Exam: **100**

Unit - I INTRODUCTION
Signals and Signal Processing, Characterization and Classification of Signals, Typical Signal Processing operations, Example of typical Signals, Case Studies: Typical Signal Processing Applications.

Unit - II TIME DOMAIN REPRESENTATION OF SIGNALS & SYSTEMS
Discrete Time Signals, Operations on Sequences, Linear shift-invariant systems, Stability and Causality, Linear Constant Coefficient Difference Equations, Frequency Domain representation of Discrete-time systems, Symmetry properties of the Fourier transform, Sampling of Continuous-time systems, Z-transforms, Inverse Z-transform, Properties of Z-transform and its applications in System Analysis & Design, Discrete Fourier Transform (DFT) & its properties, Computation of the DFT of real sequences, Linear Convolution using the DFT, Discrete Wavelet Transform (DWT), Continuous Wavelet Transform (CWT), Chirplet Transform.

Unit – III FUNDAMENTALS OF IMAGE PROCESSING
Introduction, Fundamental Steps in Image Processing, Elements of Digital Image Processing Systems, Image Sampling and Quantization, Image Enhancement in the Spatial Domain, Basics of Spatial Filters, Smoothening and Sharpening Spatial Filters, Combining Spatial Enhancement Methods, Image Enhancement in the Frequency Domain, Introduction to Fourier Transform and the frequency Domain, Smoothing and Sharpening, Frequency Domain Filters, Homomorphic Filtering, Image Restoration.

Unit – IV IMAGE ENHANCEMENT AND SEGMENTATION
Image Compression, Coding, Inter-pixel and Psycho-visual Redundancy, Image Compression Models, Elements of Information Theory, Error free (lossless) compression, Lossy compression, Image compression standards. Image Segmentation, Detection of Discontinuities, Edge linking and boundary detection, Thresholding, Region Oriented Segmentation, Motion based Segmentation.

Unit – V MORPHOLOGICAL IMAGE PROCESSING
Boundary Descriptors, Regional Descriptors, Use of Principal Components for Description, Introduction to Morphology, Some basic Morphological Algorithms. Object Recognition, Patterns and Pattern Classes, Decision - Structural Methods and Template Matching methods.

Text Books :
1. Rafael C. Gonzalez & Richard E. Woods, "Digital Image Processing", Pearson Education, 2nd edition, 2004.
2. Alan V. Oppenheim & Ronald W. Schafer, "Digital Signal Processing", PHI, 2002.

Reference Books :
1. A.K. Jain, "Fundamentals of Digital Image Processing", PHI, 2003.
2. Sanjit K Mitra, "Digital Signal Processing: A Computer Based Approach", TMH, 2nd Edition, 2003.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1ˢᵗ
Subject: **Data Encryption and Compression (Elective-I)**
Total Theory Periods: **40**
Minimum number of Class tests to be conducted: 02

Branch: **Information Security**
Code: **571131 (22)**
Total Tutorial Periods: **12**
Total Marks in End Semester Exam: **100**

Unit - I OVERVIEW OF DATA ENCRYPTION TECHNIQUES
Need for security, Security approaches, Principles of security, Types of attacks, Encryption Techniques: Plain text, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key Range & Size.

Unit - II SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION
Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital Signature, Knapsack Algorithm, User Authentication Mechanism: Authentication basics, Passwords, Authentication Tokens, Certificate based & Biometric Authentication, Firewall.

Unit – III SOFTWARE MECHANISMS ON ENCRYPTION
Denial of Service Attacks, IP Spoofing Attacks, Secure Inter branch payment transactions, Conventional Encryption and Message Confidentiality, Conventional Encryption Principles, Conventional Encryption Algorithms, Location of Encryption Devices, Key Distribution.

Unit – IV MESSAGE AUTHENTICATION AND DATA COMPRESSION MANAGEMENT
Public Key Cryptography and Message Authentication Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital Signatures, Key Management Introduction, Need for data compression, Fundamental concept of Data Compression & Coding, Communication Model, Compression Ratio, Requirements of Data Compression, Classification.

Unit - V METHODS OF DATA COMPRESSION
Data Compression- Loss Less & Lossy, Entropy Encoding - Repetitive Character Encoding, Run Length Encoding, Zero/Blank Encoding; Statistical Encoding- Huffman, Arithmetic & Lempel-Ziv Coding, Source Encoding, Vector Quantization (Simple Vector Quantization & with Error term), Differential Encoding, Predictive Coding, Differential Pulse Code Modulation (DPCM), Delta Modulation (DM), Adaptive Differential Pulse Code Modulation (ADPCM), Transform based Coding: Discrete Cosine Transform (DCT) & JPEG standards, Fractal Compression.

Text / Reference Books :
1. B. Forouzan, "Cryptography and Network Security", McGraw-Hill, 2001.
2. Nelson, "The Data Compression Book", BPB publications, 2002.
3. Atul Kahate, "Cryptography & Network Security", TMH, 2001.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st   Branch: **Information Security**
Subject: **Information Theory and Coding (ELECTIVE – I)**   Code: **571132 (22)**
Total Theory Periods: **40**   Total Tutorial Periods: **12 hours**
Minimum number of Class tests to be conducted: 02   Total Marks in End Semester Exam: **100**

Unit- I SOURCE CODING

Introduction to information theory, Uncertainty and information, Average Mutual information and entropy, Source Coding Theorem, Shannon-Fano Coding, Huffman Coding, Arithmetic Coding, Lempel-Ziv Algorithm, Run-length Encoding and Rate Distortion Function.

Unit-II CHANNEL CAPACITY AND CODING

Channel models, Channel capacity, Channel coding, Information capacity theorem, Random selection of codes, Error control coding, Linear block codes and their properties, Decoding of linear block code, Perfect codes, Hamming codes, Optimal linear codes and MDS codes.

Unit-III CYCLIC CODES

Polynomials, Division algorithm for polynomials, A method for generating cyclic codes, Matrix description of cyclic codes, Burst Error Correction, Fire codes, Golay codes, CRC codes, Circuit implementation of cyclic codes. BCH codes, Minimal polynomials, Generator polynomial for BCH codes, Decoding of BCH codes, Reed-Solomon codes and nested codes.

Unit-IV CONVOLUTION CODES

Tree codes and trellis codes, Polynomial description of convolutional codes, Distance notions for convolutional codes, Generation function, Matrix description of convolutional codes, Viterbi decoding of convolutional codes, Distance bounds for convolutional codes, Turbo codes and Turbo decoding.

Unit-V TRELLIS CODED MODULATION

Concept of coded modulation, Mapping by set partitioning, Gottfried Ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

Text / Reference Books :

1. Ranjan Bose, "Information theory: Coding and Cryptography", Tata McGraw Hill, 2002.
2. Viterbi, "Information Theory and Coding", McGraw Hill, 1982.
3. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.
4. Katre, J. S., "Information Theory and Coding Techniques", 2nd Revised Edition, Tech-Max, Pune.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Unit - I OVERVIEW OF CELLULAR SYSTEMS

A basic cellular system, Performance criteria, Uniqueness of mobile radio environment, Operation of cellular systems, Planning a cellular system, Overview of generations of cellular systems, Elements of Cellular Radio, Systems Design and Interference, General description of the problem, Concept of frequency reuse channels, Co-channel Interference reduction factor, Desired C/I from a normal case in an Omni-directional antenna system, Cell splitting, Consideration of the components of cellular systems, Introduction to co-channel interference, Co-channel measurement design of antenna system, Antenna parameter and their effects.

Unit - II MOBILE SIGNAL COVERAGES AND PROPOGATION LOSS MEDIUMS

Cell Coverage for Signal & antenna structures, General introduction, Obtaining the mobile point to point mode, Propagation over water or flat open area, Foliage loss, Propagation in near distance, Long distance propagation, Point-to-Point prediction model- Characteristics, Cell site, Antenna heights and Signal coverage cells, Mobile to mobile propagation. Characteristics of basic antenna structures, Antenna at cell site, Mobile antenna.

Unit – III CHANNEL UTILIZATION AND ITS MANAGEMENT

Frequency Management & Channel Assignment, Hand-Off & Dropped-Calls Frequency Management, Fixed channel assignment, Non-fixed channel assignment, Traffic & channel assignment, Why hand off ?, Types of handoff and their characteristics, Dropped call rates & their evaluation.

Unit – IV ERROR DETECTION AND CORRECTION MECHANISMS

Modulation methods and coding for error detection and correction, Introduction to Digital Modulation techniques, Modulation methods in cellular wireless systems, OFDM, Block Coding, Convolution Coding and Turbo coding, Multiple Access Techniques: FDMA, TDMA, CDMA, Time-Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), CDMA capacity, Probability of bit error considerations, CDMA compared with TDMA.

Unit – V CASE STUDIES ON CELLULAR SYSTEMS

Second generation digital wireless systems, GSM, IS-136 (D-AMPS), IS-95, Mobile Management, Voice Signal processing and coding.

Text Books :
1. William, C Y Lee, "Mobile Cellular Telecommunications", 2nd Edition McGraw Hill, 2002.
2. Mischa Schwartz, "Mobile Wireless Communications", Cambridge University Press, 2005.

Reference Books :
1. Theodore S Rapport, "Wireless Communication Principles and Practice", 2nd Edition Pearson Education, 2002.
2. Lawrence Harte, "3G Wireless Demystified", McGraw Hill publication, 2002.
3. Kaveh Pahlavan and Prashant Krishnamurthy, "Principles of Wireless Networks", PHI, 2000.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1ˢᵗ   Branch: **Information Security**
Subject: **Operating System Security Lab.**   Code: **571121 (22)**
Theory Periods: Nil   Total Lab Periods: **40**
Total Marks in End Semester Exam: **75**

List of Experiments :

1. Write a shell script to scan current operating system security settings.

2. Write a program to create a secured pipe for Inter-Process Communication.

3. Identify Vulnerabilities (Potential Threats) of Operating System and Security features.

4. Identify and analyze Buffer overflow problem.

5. Write a Perl Script to identify and remove root kits.

6. Write a Perl Script to analyze TCP dump for identification of worms.

7. Write a program to implement Bankers Algorithm.

8. Write a program to avoid deadlocks.

9. Write a menu driven program to implement Disk Scheduling techniques.

10. Write a program to implement semaphores.

11. Write a program for file protection.

Text / Reference Books :

1. William Stallings, "Operating systems: Internal and Design Principles", PHI, Fifth Edition, 2005.
2. Maurice J. Bach, "The Design of the Operating System", PHI, 1991.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 1st   Branch: **Information Security**
Subject: **Digital Signal and Image Processing Lab.**   Code: **571122 (22)**
Theory Periods: Nil   Total Lab Periods: **40**
Total Marks in End Semester Exam: **75**

List of Experiments :

1. **Study and Analyze important Signal Processing and Statistics toolbox functions with at least two types of Signals.**
2. Write a Matlab Code for the implementation of Convolution theorem and its applications.
3. Write a Matlab Code for the observation of frequency response and phase response of the signal.
4. Repeat the above problem for the following cases :
    a) Human Speech (Male).
    b) Human Speech (Female).
    c) Human Speech (Child).
5. Write a Matlab code to observe the Impulse response of different types of signals.
6. Write a Matlab code to implement DFT and FFT of any type of signal.
7. Write a Matlab code to implement DWT and CWT of any type of signal.
8. Write a Matlab code to implement DCT of any type of signal.
9. Write a Matlab code of the detection and counting Zero-Crossings of Speech Signal.
10. Write a Matlab code for the study of all types of Windowing techniques and its performance measures over any signal.
11. Write a Matlab program for the study and analysis of different Biometrical Signal traits of Human being for the gender, age, and prosodic features.
12. **Study and Analyze important Image Processing toolbox functions with at least two standard images like Cameraman, Lena, Monkey, and others.**
13. Write a Matlab Code 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.
14. Write a Menu driven program for implementing the following :
    a. Converting Color to Gray Scale and hence enhancement with segmentation.
    b. Color Image enhancement and Segmentation.
    c. Comparison of the above two options through Histogram plotting.
    d. Quit with a dialog box for confirmation of yes and No command button.
15. Write a program to hide a word in an image file and retrieve it (Stegnography).
16. Write a Menu driven program for the study and analysis of different Biometrical Images like Iris, finger print, Human Gait, Human face (frontal), Human face (from Side-view), Human face (temporal view) and any other Biometrical traits for the implementation of enhancement, segmentation, and features extraction.
17. Case studies through Matlab on the following :
    a) Mapping process for Trained and Test Speech Signal.
    b) Mapping process for Trained and Test Images.

Text / Reference Books :

1. Rafael C. Gonzalez & Richard E. Woods, "Digital Image Processing using Matlab", 2nd edition, Pearson Education, 2004.
2. Vinay K. Ingle, "Digital Signal Processing through Matlab", PHI, 2005.
3. A.K. Jain, "Fundamentals of Digital Image Processing", PHI, 2003.
4. Alan V. Oppenheim & Ronald W. Schafer, " Digital Signal Processing", PHI, 2002.