ME (Information Technology) with Specialization in Information Security
Proposed Scheme for CBCS (Full Time)

SEM I				
S.NO	**Sub Code**	**Sub Name**	**Number of Credit L-T-P**	**Sub Type**
1.	ISR1C1	Advanced Algorithms	3-1-1	PC1
2.	ISR1C2	Secure Computing Techniques	3-1-1	PC2
3.	ISR1C3	Advanced Computer Networks	3-1-1	PC3
4.	ISR1Gx	Generic Elective I	3-1-0	GE1
5.	ISR1Ex	Elective I	3-1-1	PE1
6.	ASR1S1	Soft Skills -1	2-0-0	
7.	ISR1W1	Seminar/ Workshop-I	0-2-0	
8.	ISR1V1	Comprehensive Viva I	0-0-4	
Total Credit for SEM I			**28 actual + 4 Virtual credits**	
		List of Generic Elective I	**L-T-P**	
1.	ISR1G1	Advanced Data Base Management Systems	3-1-0	
2.	ISR1G2	Complexity of Security Algorithms	3-1-0	
3.	ISR1G3	Agent Technology	3-1-0	
		List of Elective I	**L-T-P**	
1.	ISR1E1	Data Security	3-1-1	
2.	ISR1E2	Information Theory and Coding	3-1-1	
3.	ISR1E3	Data Compression and Stagnography	3-1-1	
SEM II			**L-T-P**	
1.	ISR2C1	Information Security Management	3-1-1	PC4
2.	ISR2C2	Digital Forensics and Security Audit	3-1-1	PC5
3.	ISR2C3	Secure Wireless Networks	3-1-1	PC6
4.	ISR2Gx	Generic Elective II	3-1-0	GE2
5.	ISR2Ex	Elective II	3-1-1	PE2
6.	ASR2S2	Soft Skills -2	2-0-0	
7.	ISR2W2	Seminar/ Workshop-II	0-2-0	
8.	ISR2V2	Comprehensive Viva II	0-0-4	
Total Credit for SEM II			**28 actual + 4 Virtual credits**	
		List of Generic Elective II	**L-T-P**	
1.	ISR2G1	Cloud Computing	3-1-0	
2.	ISR2G2	Applied Cryptography	3-1-0	
3.	ISR2G3	Cyber Crime and Information Warfare	3-1-0	
		List of Elective II	**L-T-P**	
1.	ISR2E1	Biometric Systems & Security	3-1-1	
2.	ISR2E2	Secure Software Engineering	3-1-1	
3.	ISR2E3	Trust management in E- Commerce	3-1-1	
SEM III	ISR3D1	Dissertation Phase I	0-0-12	
	ISR3V3	Comprehensive Viva III	0-0-4	
Total Credit for SEM III			**12 actual + 4 Virtual credits**	
SEM IV	ISR3D2	Dissertation Phase II	0-0-12	
	ISR4V4	Comprehensive Viva IV	0-0-4	
Total Credit for SEM IV			**12 actual + 4 Virtual credits**	
Total Credit			**80 actual + 16 Virtual credits**	

ME (Information Technology) with Specialization in Information Security
Proposed Scheme for CBCS (Part Time)

SEM I				
S.NO	Sub Code	Sub Name	Number of Credit **L-T-P**	SubType
1.	ISP1C1	Advanced Algorithms	3-1-1	PC1
2.	ISP1C2	Secure Computing Techniques	3-1-1	PC2
3.	ISP1Gx	Generic Elective I	3-1-0	GE1
4.	ISP1V1	Comprehensive Viva I	0-0-2	
Total Credit for SEM I			**14 actual + 2 Virtual credits**	
SEM II			**L-T-P**	
1.	ISP2C3	Advanced Computer Networks	3-1-1	PC3
2.	ISP2EX	Elective I	3-1-1	PE1
3.	ISP2W1	Seminar/ Workshop-I	0-2-0	
4	ISP2V2	Comprehensive Viva II	0-0-2	
5.	ASP2S1	Soft Skills-1	2-0-0	
Total Credit for SEM II			**14 actual + 2 Virtual credits**	
		List of Generic Elective I	**L-T-P**	
1.	ISP1G1	Advanced Data Base Management Systems	3-1-0	
2.	ISP1G2	Complexity of Security Algorithms	3-1-0	
3.	ISP1G3	Agent Technology	3-1-0	
		List of Elective I	**L-T-P**	
1**.**	ISP2E1	Data Security	3-1-1	
2.	ISP2E2	Information Theory and Coding	3-1-1	
3.	ISP2E3	Data Compression and Stagnography	3-1-1	
SEM III			**L-T-P**	
1.	ISP3C1	Information Security Management	3-1-1	PC4
2.	ISP3C2	Digital Forensics and Security Audit	3-1-1	PC5
3.	ISP3Gx	Generic Elective II	3-1-0	GE2
4.	ISP3V3	Comprehensive Viva III	0-0-2	
Total Credit for SEM III			**14 actual + 2 Virtual credits**	
SEM IV			**L-T-P**	
1.	ISP4C3	Secure Wireless Networks	3-1-1	PC6
2.	ISP4Ex	Elective II	3-1-1	PE2
3.	ISP4W2	Seminar/ Workshop-II	0-2-0	
4.	ISP4V4	Comprehensive Viva IV	0-0-2	
5.	ASP4S2	Soft Skills-2	2-0-0	
Total Credit for SEM IV			**14 actual + 2 Virtual credits**	
		List of Generic Elective II	**L-T-P**	
1.	ISP3G1	Cloud Computing	3-1-0	
2.	ISP3G2	Applied Cryptography	3-1-0	
3.	ISP3G3	Cyber Crime and Information Warfare	3-1-0	
		List of Elective II	**L-T-P**	
1.	ISP4E1	Biometric Systems & Security	3-1-1	
2.	ISP4E2	Secure Software Engineering	3-1-1	
3.	ISP4E3	Trust management in E- Commerce	3-1-1	
SEM V				
ISP5D1		Dissertation Phase I	0-0-12=12	
ISP5V5		Comprehensive Viva V	0-0-4=4	
Total Credit for SEM V			**12 actual + 4 Virtual credits**	

SEM VI			
ISP6D2	Dissertation Phase II	0-0-12=12	
ISP6V6	Comprehensive Viva VI	0-0-4=4	
Total Credit for SEM VI		**12 actual + 4 Virtual credits**	
Total Credit		**80 actual + 16 Virtual credits**	

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1C1: Advanced Algorithms	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

To introduce students a variety of advanced techniques, methods and results from the rapidly-developing field of algorithms to solve problems. To familiarise the state of the art in some areas of algorithmic research, including open problems.

COURSE CONTENT

Unit I

Review of basic concepts; Worst case and average case analysis, Asymptotic notation, Solving recurrence equations, Medians and order statistics, Advanced data structures: Binomial Heaps, Fibonacci Heaps, Data Structures for Disjoint Sets – Disjoint-set operations, Linked-list representation of disjoint sets, Disjoint-set forests, analysis of union by rank with path compression.

Unit II

Advanced Design and Analysis techniques: Greedy and Dynamic Programming strategies, Backtracking, Branch and Bound. Algorithms for Knapsack problems, Matrix-Chain Multiplication problem, Travelling Salesperson Problem (TSP), etc. Amortized analysis: the aggregate method, the accounting method, the potential method, Dynamic tables.

Unit III

Graph algorithms: Breadth-first search, Depth-first search, Topological sorting, Minimum Spanning Trees, Single-Source Shortest Paths, All-Pairs Shortest Paths, Maximum Flows: Augmenting Paths and Push-Relabel Methods, Minimum Cost Flows, Bipartite Matching.

Unit IV

Graph algorithms: Breadth-first search, Depth-first search, Topological sorting, Minimum Spanning Trees, Single-Source Shortest Paths, All-Pairs Shortest Paths, Maximum Flows: Augmenting Paths and Push-Relabel Methods, Minimum Cost Flows, Bipartite Matching.

Unit V

Theory of NP-Hard and NP-Complete Problems: P, NP and NP-Complete complexity classes; A few NP-Completeness proofs; other complexity classes.

Dealing with intractability: Introduction, Combinatorial Optimization, approximation factor, PTAS, FPTAS, Approximation algorithms for vertex cover, set cover, TSP, knapsack, bin packing, subset-sum problem etc. Analysis of the expected time complexity of the algorithms.

Text and Reference books:

[1] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. Introduction to Algorithms. (3rd Ed). MIT Press, McGraw-Hill, 2010.

[2] M.T. Goodrich, R. Tamassia, “Algorithm design – Foundations, Analysis, and Internet Examples”, John Wiley, Second Edition.

[3] V. V. Vazirani, Approximation Algorithms, Springer. 2001.

[4] Ravindra K. Ahuja, Thomas L. Magnanti, and James B. Orlin, Network Flows: Theory, Algorithms, and Applications,

[5] E Horrowitz, S salmi, S Rajasekaran, “Fundamentals of Computer Algorithms”, Second Edition, University Press, 2007.

[6] Aho, A V Hopcraft Ullman JD, “The Design and analysis of computer Algorithms”, Pearson Education, 2007.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1C2: Secure Computing Techniques	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

COURSE CONTENT

Unit-I: Introduction

Security: CIA (AIC) Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. *Malware Terminology*: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks, IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. *Types of Security Vulnerabilities*: buffer overflows, invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit-II: Secure Software Development Cycle & Threat Modelling

Need for Secure Systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Unit – III: Secure Coding Techniques

Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, *Insecure Coding Practices in Java Technology*: ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. *Security Issues in C/C++ Language*: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM. Secure coding issues in Android Applications, Language Specific issues like C/C++, Perl, Python, Scripting Languages, Ada, Java, PHP etc.

Unit – IV: Database and Web-specific issues

SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

Unit – V: Testing Secure Applications

Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

Text and Reference books:

[1] Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004

[2] Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress,1st Edition, 2005

[3] Threat Modeling, Frank Swiderski and Window Snyder, Microsoft Professional, 1st Edition, 2004.

[4] Secure Programming HOWTO by David A. Wheeler

[5] Secure Coding: Principles & Practices by Mark G. Graff, Kenneth R. van Wyk

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1C3: Advanced Computer Networks	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

Provide students with enhance base of knowledge of Computer Networks, Develop a comprehensive knowledge of Tools and Techniques used in Management of Computer Networks, Develop skills in independent managing Network Performance related issues Develop ability to carry out research in area of Computer Networks

COURSE CONTENT

Unit I : Foundation

Computer Networks and Internet, Structure of network software in an operating system, Packet Switching and Circuit Switching, Protocols Layers and Network Service Models, Implementing Network Software (Sockets), Network Performance - Delay, Loss , Throughput, and Bandwidth, Best-effort services and QoS guarantees for multimedia data.

Unit II : Link Layer, Access Networks and LANs

Services Provided by Link Layer, Link Layer Implementation, Multiple Access Protocols and Ethernet, Switched Local Area Networks, Link Layer Addressing (ARP), RARP, VLANS, Link Virtualization and MPLS, Data Center Networking

Unit III : Network Layer and Internetworking

Virtual Circuit and Datagram Networks, Internet Protocol, IPV4 -Class full and Classless Addressing, Subnetting, IPV6 Addressing, IP Datagram delivery and forwarding, Routing Algorithms- Distance Vector and RIP, Link State Routing and OSPF, Inter domain Routing - BGP, DHCP, ICMP, Router-switching, input/output processing, Routing Control Plane, Network Virtualization- VPN and NAT.

Unit IV : Transport Layer and End-to-End Protocols

Transport layer services in Internet, Multiplexing and De-multiplexing, Connectionless Transport: UDP segment format and checksum, Connection Oriented Transport: TCP-segment format, roundtrip estimation and Timeout, Reliable data Transfer, Flow control, TCP connection Management, TCP congestion control Additive Increase/Multiplicative Decrease, Slow start, Fast Retransmit and Fast Recovery, Fairness and Queuing Disciplines.

Unit V : Application Layer

Network Application Architecture and Process Communication, Web and HTTP, File Transfer FTP, Electronic Mail- SMTP, POP, IMAP, MIME, Internet Discovery Service-DNS, Network Management – SNMP, Advance topics - Software Defined Networking, Internet of Things

Text and Reference books:

[1] Computer Networking, A Top-Down Approach, 6th Ed., J. Kurose and K. Ross, Pearson, 2013.

[2] Computer Networks, A Systems Approach, 5th Edition, L. Peterson and B. Davie, Morgan Kaufman, 2012.

[3] Internetworking with TCP/IP Volume I, 6th Ed., D. E. Comer, Pearson Education, 2013.

[4] Internetworking with TCP/IP Volume II, 3rd, Ed., D. E. Comer and David L. Stevens, Pearson Education, 2003.

[5] Data Communications and Networking, 4th Ed., Beharouz A. Forouzan, McGraw-Hill Education Private Ltd., 2006.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1G1: Advanced Database Management Systems	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**0**	**3**	**1**	**0**	**4**

Course Objective:
To enhance the understanding of practical issues related to advance topics of Database systems.

COURSE CONTENT

Unit I : Introduction to Data Warehousing and Data Mining
Introduction to Knowledge discovery process, OLTP, OLAP, Data Mining: Functionalities, Process, Schemas and Applications etc.; Data Warehouse : Construction and other issues.

Unit II : Transaction Processing and Concurrency Control
Introduction, Properties; Schedules, Types of Schedules, Characterizing Schedules, Serializability, Two-phase locking, Dealing with Deadlock and Starvation, Time Stamp Ordering and Multi version Concurrency control etc.

Unit III : Data Storage, Indexing and Physical Database Design
Types of Files, Introduction to Hashing, Multilevel Indexes, B-trees, B+ -trees, Indexes on Multiple Keys, Overview of Physical Database Design and Database Tuning in Relational Databases

Unit IV : Query Optimization
Introduction to Query Optimization, Overview of algorithms used in External Sorting and other SQL operations, Use of Heuristics, Cost Estimation and Selectivity used in Query Optimization, Semantic Query Optimization etc.

Unit V : Distributed Databases and Security
Concepts, Types and Query Processing in Distributed Databases, Data Fragmentation, Replication and Allocation Techniques, Introduction to Database Security Issues, Access Control Policy, Statistical Database Security etc.

Text and Reference books:

[1] Fundamentals of Database Systems, Elmasri and Navathe, Pearson Education, 6th Edition, 2014.
[2] Data Mining Concepts and Techniques, Han and Kamber, Morgan Kauffman, 3rd Edition, India, 2012.
[3] Database System Concepts, Silberchatz, Korth, Sudarshan, Mcgraw Hill, 6th Edition, 2010.
[4] Database Systems : A practical Approach to Design, Implementation, and Management, Connolly and Begg, Pearson Education, 6th Edition, 2014.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR1E1: Data Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:
To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

COURSE CONTENT

Unit I : Foundation
Security Taxonomy, Domain of information security, security goals, security approaches, principles of security, security attacks, threats, vulnerabilities, malicious software's, virus, worms, Trojan, spy wares, Applets/Active X, cookies. Security services, mechanisms and security models. Types of attacks, packet sniffing, packet spoofing, IP sniffing, IP spoofing, DNS spoofing attack.

Unit II : Classical Cryptographic Techniques
Cryptography terminologies, classical cryptography: substitution techniques, transposition techniques, playfair cipher, Hill cipher. Mathematics of cryptography: Integer arithmetic, modular arithmetic, Elucid theorem, Concept of symmetric and asymmetric key cryptography, stenography, digital watermarking, key range and size, possible types of attacks. Stream ciphers and Block cipher. Algorithm type and modes. Key distribution, Deffie Hellman key exchange, Man in the middle attack.

Unit III : Symmetric Key Algorithms
Computer based symmetric key cryptographic algorithms: Data Encryption Standard (DES), Double DES, meet in the middle attack, Triple DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, Advance Encryption Standard (AES).

Unit IV : Asymmetric Key Algorithms
Random number generation, Prime numbers. Fermat's and Euler's theorem. Principles of public key crypto systems. Computer based asymmetric key cryptographic algorithms: RSA algorithm. Principles of public key cryptosystems, symmetric and asymmetric key cryptography together. Concept of Digital Envelope, Digital signatures, message digests and its requirements.

Unit V : Public Key Crptosystems
MD5 Message Digest Algorithm, Message authentic codes, Hash functions, Secure Hash Algorithms, Hash based message authentic code. Elliptical Curve Cryptography (ECC). Problems with the public key exchange.

Text and Reference books:

[1] Douglas R. Stinson;"Cryptography Theory and Practice"; Chapman & Hall/CRC
[2] Williams Stallings; "Cryptography & Network Security"; Pearson Education.
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley
[4] Atul Kahate; "Cryptography and Network Security"; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP1C1: Advanced Algorithms	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

To introduce students a variety of advanced techniques, methods and results from the rapidly-developing field of algorithms to solve problems. To familiarise the state of the art in some areas of algorithmic research, including open problems.

COURSE CONTENT

Unit I

Review of basic concepts; Worst case and average case analysis, Asymptotic notation, Solving recurrence equations, Medians and order statistics, Advanced data structures: Binomial Heaps, Fibonacci Heaps, Data Structures for Disjoint Sets – Disjoint-set operations, Linked-list representation of disjoint sets, Disjoint-set forests, analysis of union by rank with path compression.

Unit II

Advanced Design and Analysis techniques: Greedy and Dynamic Programming strategies, Backtracking, Branch and Bound. Algorithms for Knapsack problems, Matrix-Chain Multiplication problem, Travelling Salesperson Problem (TSP), etc. Amortized analysis: the aggregate method, the accounting method, the potential method, Dynamic tables.

Unit III

Graph algorithms: Breadth-first search, Depth-first search, Topological sorting, Minimum Spanning Trees, Single-Source Shortest Paths, All-Pairs Shortest Paths, Maximum Flows: Augmenting Paths and Push-Relabel Methods, Minimum Cost Flows, Bipartite Matching.

Unit IV

Graph algorithms: Breadth-first search, Depth-first search, Topological sorting, Minimum Spanning Trees, Single-Source Shortest Paths, All-Pairs Shortest Paths, Maximum Flows: Augmenting Paths and Push-Relabel Methods, Minimum Cost Flows, Bipartite Matching.

Unit V

Theory of NP-Hard and NP-Complete Problems: P, NP and NP-Complete complexity classes; A few NP-Completeness proofs; other complexity classes.

Dealing with intractability: Introduction, Combinatorial Optimization, approximation factor, PTAS, FPTAS, Approximation algorithms for vertex cover, set cover, TSP, knapsack, bin packing, subset-sum problem etc. Analysis of the expected time complexity of the algorithms.

Text and Reference books:

[1] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. Introduction to Algorithms. (3rd Ed). MIT Press, McGraw-Hill, 2010.

[2] M.T. Goodrich, R. Tamassia, “Algorithm design – Foundations, Analysis, and Internet Examples”, John Wiley, Second Edition.

[3] V. V. Vazirani, Approximation Algorithms, Springer. 2001.

[4] Ravindra K. Ahuja, Thomas L. Magnanti, and James B. Orlin, Network Flows: Theory, Algorithms, and Applications,

[5] E Horrowitz, S salmi, S Rajasekaran, “Fundamentals of Computer Algorithms”, Second Edition, University Press, 2007.

[6] Aho, A V Hopcraft Ullman JD, “The Design and analysis of computer Algorithms”, Pearson Education, 2007.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP1C2: Secure Computing Techniques	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

COURSE CONTENT

Unit-I: Introduction

Security: CIA (AIC) Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. *Malware Terminology*: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks, IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. *Types of Security Vulnerabilities*: buffer overflows, invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit-II: Secure Software Development Cycle & Threat Modelling

Need for Secure Systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Unit – III: Secure Coding Techniques

Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, *Insecure Coding Practices in Java Technology*: ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. *Security Issues in C/C++ Language*: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM. Secure coding issues in Android Applications, Language Specific issues like C/C++, Perl, Python, Scripting Languages, Ada, Java, PHP etc.

Unit – IV: Database and Web-specific issues

SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

Unit – V: Testing Secure Applications

Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.

Text and Reference books:

[1] Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004
[2] Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress,1st Edition, 2005
[3] Threat Modeling, Frank Swiderski and Window Snyder, Microsoft Professional, 1st Edition, 2004.
[4] Secure Programming HOWTO by David A. Wheeler
[5] Secure Coding: Principles & Practices by Mark G. Graff, Kenneth R. van Wyk

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP2C3: Advanced Computer Networks	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

Provide students with enhance base of knowledge of Computer Networks, Develop a comprehensive knowledge of Tools and Techniques used in Management of Computer Networks, Develop skills in independent managing Network Performance related issues Develop ability to carry out research in area of Computer Networks

COURSE CONTENT

Unit I : Foundation

Computer Networks and Internet, Structure of network software in an operating system, Packet Switching and Circuit Switching, Protocols Layers and Network Service Models, Implementing Network Software (Sockets), Network Performance - Delay, Loss , Throughput, and Bandwidth, Best-effort services and QoS guarantees for multimedia data.

Unit II : Link Layer, Access Networks and LANs

Services Provided by Link Layer, Link Layer Implementation, Multiple Access Protocols and Ethernet, Switched Local Area Networks, Link Layer Addressing (ARP), RARP, VLANS, Link Virtualization and MPLS, Data Center Networking

Unit III : Network Layer and Internetworking

Virtual Circuit and Datagram Networks, Internet Protocol, IPV4 -Class full and Classless Addressing, Subnetting, IPV6 Addressing, IP Datagram delivery and forwarding, Routing Algorithms- Distance Vector and RIP, Link State Routing and OSPF, Inter domain Routing - BGP, DHCP, ICMP, Router-switching, input/output processing, Routing Control Plane, Network Virtualization- VPN and NAT.

Unit IV : Transport Layer and End-to-End Protocols

Transport layer services in Internet, Multiplexing and De-multiplexing, Connectionless Transport: UDP segment format and checksum, Connection Oriented Transport: TCP-segment format, roundtrip estimation and Timeout, Reliable data Transfer, Flow control, TCP connection Management, TCP congestion control Additive Increase/Multiplicative Decrease, Slow start, Fast Retransmit and Fast Recovery, Fairness and Queuing Disciplines.

Unit V : Application Layer

Network Application Architecture and Process Communication, Web and HTTP, File Transfer FTP, Electronic Mail- SMTP, POP, IMAP, MIME, Internet Discovery Service-DNS, Network Management – SNMP, Advance topics - Software Defined Networking, Internet of Things

Text and Reference books:

[1] Computer Networking, A Top-Down Approach, 6th Ed., J. Kurose and K. Ross, Pearson, 2013.

[2] Computer Networks, A Systems Approach, 5th Edition, L. Peterson and B. Davie,Morgan Kaufman, 2012.

[3] Internetworking with TCP/IP Volume I, 6th Ed., D. E. Comer, Pearson Education, 2013.

[4] Internetworking with TCP/IP Volume II, 3rd, Ed., D. E. Comer and David L. Stevens, Pearson Education, 2003.

[5] Data Communications and Networking, 4th Ed., Beharouz A. Forouzan, McGraw-Hill Education Private Ltd., 2006.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME I Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP1G1: Advanced Database Management Systems	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**0**	**3**	**1**	**0**	**4**

Course Objective:
To enhance the understanding of practical issues related to advance topics of Database systems.

COURSE CONTENT

Unit I : Introduction to Data Warehousing and Data Mining
Introduction to Knowledge discovery process, OLTP, OLAP, Data Mining: Functionalities, Process, Schemas and Applications etc.; Data Warehouse : Construction and other issues.

Unit II : Transaction Processing and Concurrency Control
Introduction, Properties; Schedules, Types of Schedules, Characterizing Schedules, Serializability, Two-phase locking, Dealing with Deadlock and Starvation, Time Stamp Ordering and Multi version Concurrency control etc.

Unit III : Data Storage, Indexing and Physical Database Design
Types of Files, Introduction to Hashing, Multilevel Indexes, B-trees, B+ -trees, Indexes on Multiple Keys, Overview of Physical Database Design and Database Tuning in Relational Databases

Unit IV : Query Optimization
Introduction to Query Optimization, Overview of algorithms used in External Sorting and other SQL operations, Use of Heuristics, Cost Estimation and Selectivity used in Query Optimization, Semantic Query Optimization etc.

Unit V : Distributed Databases and Security
Concepts, Types and Query Processing in Distributed Databases, Data Fragmentation, Replication and Allocation Techniques, Introduction to Database Security Issues, Access Control Policy, Statistical Database Security etc.

Text and Reference books:

[1] Fundamentals of Database Systems, Elmasri and Navathe, Pearson Education, 6th Edition, 2014.
[2] Data Mining Concepts and Techniques, Han and Kamber, Morgan Kauffman, 3rd Edition, India, 2012.
[3] Database System Concepts, Silberchatz, Korth, Sudarshan, Mcgraw Hill, 6th Edition, 2010.
[4] Database Systems : A practical Approach to Design, Implementation, and Management, Connolly and Begg, Pearson Education, 6th Edition, 2014.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- A			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP2E1: Data Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:
To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

COURSE CONTENT

Unit I : Foundation
Security Taxonomy, Domain of information security, security goals, security approaches, principles of security, security attacks, threats, vulnerabilities, malicious software's, virus, worms, Trojan, spy wares, Applets/Active X, cookies. Security services, mechanisms and security models. Types of attacks, packet sniffing, packet spoofing, IP sniffing, IP spoofing, DNS spoofing attack.

Unit II : Classical Cryptographic Techniques
Cryptography terminologies, classical cryptography: substitution techniques, transposition techniques, playfair cipher, Hill cipher. Mathematics of cryptography: Integer arithmetic, modular arithmetic, Elucid theorem, Concept of symmetric and asymmetric key cryptography, stenography, digital watermarking, key range and size, possible types of attacks. Stream ciphers and Block cipher. Algorithm type and modes. Key distribution, Deffie Hellman key exchange, Man in the middle attack.

Unit III : Symmetric Key Cryptography
Computer based symmetric key cryptographic algorithms: Data Encryption Standard (DES), Double DES, meet in the middle attack, Triple DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, Advance Encryption Standard (AES).

Unit IV : Asymmetric Key Cryptography
Random number generation, Prime numbers. Fermat's and Euler's theorem. Principles of public key crypto systems. Computer based asymmetric key cryptographic algorithms: RSA algorithm. Principles of public key cryptosystems, symmetric and asymmetric key cryptography together. Concept of Digital Envelope, Digital signatures, message digests and its requirements.

Unit V : Asymmetric Key Cryptosystems
MD5 Message Digest Algorithm, Message authentic codes, Hash functions, Secure Hash Algorithms, Hash based message authentic code. Elliptical Curve Cryptography (ECC). Problems with the public key exchange.

Text and Reference books:

[1] Douglas R. Stinson, "Cryptography Theory and Practice"; Chapman & Hall/CRC
[2] Williams Stallings; "Cryptography & Network Security"; Pearson Education.
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley
[4] Atul Kahate; "Cryptography and Network Security"; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2C1: Information Security Management	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

To study the methods of managing information systems in a secure way.

COURSE CONTENT

Unit I : Foundation

Computer Security, Threats to security, History of Computer security, Computer System Security and Access Controls (System access and data access). Threats - Viruses ,worms , Trojan horse, bombs, trap doors, spoofs, email virus, macro viruses, remedies, Intruders, Malicious software.

Unit II : Communication Security

Encryption, Public Key Infrastructure, Digital Signatures, Digital signatures.

Unit III : User Authentic Mechanisms

Passwords, Authentication tokens, Certificate based Authentication, Single Sign on (SSO), Kerberos, X.509, Cryptographic Solutions- A case study.

Unit IV : Information Security Protocols

Secure Socket Layer (SSL), Secure Hyper Text Transfer Protocol (SHTTP), Secure Electronic Transaction (SET), Electronic Money, Email Security.

Unit V : System and Application Security

Intrusion detection techniques, techniques to provide privacy in Internet Application and protecting digital contents(music, vedio, software) from unintended use, authentication. IP security, Web security. file System security, program and security, memory security, Sandboxing. Security threads protection intruders- Viruses-trusted system. Firewalls, vulnerabilities & threats, Network Denial of service attack, Contract Signing, Secret Splitting.

Text and Reference books:

[1] Dieter Gollman; Computer Security; John Wiley & Sons 1999
[2] Mathew Bishop; Computer Security; Art and Science; Addison-Wisley Oct. 2007
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley Oct 2004
[4] Kaufman, Perlman and Speciner; “Network security”; Pearson Education 1995.
[5] Atul Kahate; “Cryptography and Network Security”; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2C2: Digital Forensics and Security Audit	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

At the completing of the course, students will be able to understand the fundamental concepts of forensic science and digital forensics principles. Learn to identify importance of digital evidence.

COURSE CONTENT

Unit I : Introduction of Digital Forensics:

Digital crime, current scenario of digital crime in India, Evidence and its role in IT Act, Digital Evidence, Digital Vs Physical Evidence, nature of Digital Evidence, precautions while dealing with Digital Evidence, challenging aspects of Digital Evidence, Digital Devices, evidential potential of digital devices, Digital Forensics, dimensions and principles of Digital Forensics, Digital Forensic Investigation, Investigation Models, Scientific method in Digital Investigation, Research potential and scope in digital forensics.

Unit II : Data and Evidence Recovery:

Seizure of digital information : Issues, methodology, factors limiting wholesale seizure, pulling the plug or not; data objects, Storage Media, Variety of data, Recovered data objects, electronic evidence: secure boot and write blockers, disk file organization ,disk and file imaging; forensic tools, forensic data carving, data recovering techniques.

Unit III : Mobile and Live Forensics Investigations:

Mobile phone forensics: mobile device characteristics, memory considerations, tools classification, flasher boxes, obstructed devices, forensics procedures: preservation, acquisition, examination and analysis, reporting; SIM Card Forensics.

Network Forensics: sources of network based evidences, procedure for applying network based forensics, digital evidence on internet, digital evidence on physical and data link layers, digital evidence at the network and transport layers.

Unit IV : Security Issues and Principles:

Risk Analysis: Terms and Definitions, Need, Methodology, Considerations and Approaches.

Security Models: IA-CMM,ISM3, SSE-CMM: Importance, Usage, Structure and Architecture, Process Areas; Security Engineering and its need.

Security Standards and frameworks: ISO 27001: Evolution, Organizational Context, ISMS Implementation in Organizations; COBIT: Principles, Structure and Objectives.

Security Methodologies: IAM, IEM, OCTAVE, OSSTMM,SIPES.

Laws for Information Security: Introduction to The Indian IT Act, IPR, Patent law, Copyright Law.

Unit V : Security Audit/Assurance:

Security Audits : Need in Organizations, Auditor's responsibility, Types, Approaches, Technology- Based Audits : Penetration Testing and Vulnerability Scanning; Phases, Budgeting for Security Audits.

Privacy : Organizational implications, Practices ,Policy, Audits: Framework and Approach, Standards, Phases, Process : Design, Risk Analysis, Planning, Conducting, Reporting.

Text and Reference books:

[1] Nina Godbole, Information Systems Security-Security Management, Metrics, Frameworks and Best Practices, Wiley, 2009.

[2] Digital Forensics and Cyber Crime; Ibrahim Baggili; Springer.

[3] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Massachusetts, Ed. Boston: Addision Wesley, 2001.

[4] Rick Ayers, Sam Brothers and Wayne Jansen : Guidelines on Mobile Device Forensics, NIST, 2014.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2C3: Secure Wireless Networks	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

- Provide students with enhance base of knowledge of wireless networking.
- Learn Security Issues in different wireless networks and mitigation techniques
- Develop a comprehensive knowledge of Tools and Techniques used in Management of wireless Networks
- Develop ability to carry out research in area of security in wireless Networks

COURSE CONTENT

Unit I : Foundation

Review of wireless communication Technologies : Cellular Networks, Wireless LAN, Prersonal Area Networks, Adhoc and Sensor Networks, Challenges in Adhoc and Sensor networks: Constrained Resources, Security, Mobility

Unit II :

Adaptability in Mobile computing, Mobility Management: Location Management Principles and Techniques, Data Dissemination and Management.

Unit III : Mobile and Wireless Security Issues, Approaches to security, Security in Wireless Personal Area Networks: Bluetooth Security Modes, Bluetooth Security Mechanisms, Authentication and Encryption in Bluetooth networks.

Unit IV :

Security in Wireless Local Area Networks: WEP, WPA, IEEE802.11i, Security in Metropolitan Area Networks: IEEE 802.16 and Security.

Unit V :

Security in Wide Area Networks: GSM Security, Four Generations of Wireless: 1G-4G, limitations and Security. Security in Ad hoc and Sensor networks.

Text and Reference books:

[1] Fundamentals of Mobile and Pervasive Computing, Frank Adelstein, S.K. Gupta, G. Richard
[2] III, L. Schwiebert, Mc Graw Hill, Ed.2005.
[3] Hacking Exposed : Mobile Secrets & Solutions, N.Bergman, M.Stanfield, J.Rose, J. Scambray.
[4] Building Secure Wireless Networks with 802.11, Jahanzeb Khan and Anis Khwaja, Wiley 2003.
[5] Ad Hoc Wireless Networks - Architectures and Protocols, C.Siva Ram Murthy and B.S.Manoj., Prentice Hall, 2004
[6] Technical Papers.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2G2: Applied Cryptography	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**0**	**3**	**1**	**0**	**4**

Course Objective:
To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

COURSE CONTENT

Unit I : Modular Arithmetic and Multiplicative Group
Modular Arithmetic for advanced cryptography, Multiplicative group of integers „ order of an element in , generator of , extended Euclidean algorithm, Pohlig-Hellman and Pollard-Rho algorithm for computing DLP, Integer factorization problems, Pollard-Rho factoring algorithm.

Unit II : Tools for Symmetric key & Public key Cryptography
Shannon ciphers and perfect security, computational ciphers and semantic security, efficient adversaries and attack games, trapdoor function schemes, trapdoor function pair schemes, ElGamal cryptographic system, ElGamal digital signatures, fun applications.

.

Unit III : Block Ciphers and Their Attacks
Polynomial arithmetic, finite field GF(2^n), constructing block cipher in practice, sophisticated attacks on block ciphers, case study block cipher AES: AES structure, AES transformation functions, AES key expansions, AES Implementation, fun applications.

Unit IV : Cryptanalysis, IDS and Attacks
Intrusion detection system (IDS), cross site scripting attacks, SQL injection attacks, fault injection attacks, side channel attacks, algorithmic attacks.

Unit V : Asymmetric Key Cryptosystems
MD5 Message Digest Algorithm, Message authentic codes, Hash functions, Secure Hash Algorithms, Hash based message authentic code. Elliptical Curve Cryptography (ECC). Problems with the public key exchange.

Text and Reference books:

[1] Douglas R. Stinson;"Cryptography Theory and Practice"; Chapman & Hall/CRC
[2] Williams Stallings; "Cryptography & Network Security"; Pearson Education.
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley
[4] Atul Kahate; "Cryptography and Network Security"; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISR2E1: Biometric Systems & Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:
To study the concepts of various biological based information security systems.

COURSE CONTENT

Unit I : Overview of Biometrics
Definitions, biometric modalities, course outline, Basic applications: access control, e-commerce, forensics.

Unit II : Design of a Biometric System
Building blocks, Modes of operation, Fingerprint verification: Minutiae Based Fingerprint Matching, Non-minutiae Based Representations, Fingerprint Enhancement, and Fingerprint Classification. Face Recognition:- Introduction, Authentication vs. Identification, Challenges in Face recognition, Algorithms for face recognitions.
.

Unit III : Iris Recognition
Introduction, devices for capturing Iris, Iris representation schemes, Iris recognition algorithms. Biometrics based on hand geometry, signature, ear, palm, voice and DNA.

Unit IV : Multimodal Biometrics
Limitations of unimodal systems, multibiometric scenarios, levels of fusion, system design, score fusion techniques, score normalization, user-specific parameters, and soft biometrics.

Unit V : Case Study Presentations
Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim, Identification Forensic Odontology

Text and Reference books:

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar; “Handbook of Fingerprint Recognition”; Springer Verlag, 2003.
[2] A.K. Jain, R. Bolle, S. Pankanti (Eds.); “BIOMETRICS: Personal Identification in Networked Society”, Kluwer Academic Publishers, 1999.
[3] J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.); Biometric Systems: Technology, “Design and Performance Evaluation”; Springer, 2004.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP3C1: Information Security Management	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

To study the methods of managing information systems in a secure way.

COURSE CONTENT

Unit I : Foundation

Computer Security, Threats to security, History of Computer security, Computer System Security and Access Controls (System access and data access). Threats - Viruses ,worms , Trojan horse, bombs, trap doors, spoofs, email virus, macro viruses, remedies, Intruders, Malicious software.

Unit II : Communication Security

Encryption, Public Key Infrastructure, Digital Signatures, Digital signatures.

Unit III : User Authentic Mechanisms

Passwords, Authentication tokens, Certificate based Authentication, Single Sign on (SSO), Kerberos, X.509, Cryptographic Solutions- A case study.

Unit IV : Information Security Protocols

Secure Socket Layer (SSL), Secure Hyper Text Transfer Protocol (SHTTP), Secure Electronic Transaction (SET), Electronic Money, Email Security.

Unit V : System and Application Security

Intrusion detection techniques, techniques to provide privacy in Internet Application and protecting digital contents(music, vedio, software) from unintended use, authentication. IP security, Web security. file System security, program and security, memory security, Sandboxing. Security threads protection intruders- Viruses-trusted system. Firewalls, vulnerabilities & threats, Network Denial of service attack, Contract Signing, Secret Splitting.

Text and Reference books:

[1] Dieter Gollman; Computer Security; John Wiley & Sons 1999
[2] Mathew Bishop; Computer Security; Art and Science; Addison-Wisley Oct. 2007
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley Oct 2004
[4] Kaufman, Perlman and Speciner; “Network security”; Pearson Education 1995.
[5] Atul Kahate; “Cryptography and Network Security”; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP3C2: Digital Forensics and Security Audit	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

At the completing of the course, students will be able to understand the fundamental concepts of forensic science and digital forensics principles. Learn to identify importance of digital evidence.

COURSE CONTENT

Unit I : Introduction of Digital Forensics:

Digital crime, current scenario of digital crime in India, Evidence and its role in IT Act, Digital Evidence, Digital Vs Physical Evidence, nature of Digital Evidence, precautions while dealing with Digital Evidence, challenging aspects of Digital Evidence, Digital Devices, evidential potential of digital devices, Digital Forensics, dimensions and principles of Digital Forensics, Digital Forensic Investigation, Investigation Models, Scientific method in Digital Investigation, Research potential and scope in digital forensics.

Unit II : Data and Evidence Recovery:

Seizure of digital information : Issues, methodology, factors limiting wholesale seizure, pulling the plug or not; data objects, Storage Media, Variety of data, Recovered data objects, electronic evidence: secure boot and write blockers, disk file organization ,disk and file imaging; forensic tools, forensic data carving, data recovering techniques.

Unit III : Mobile and Live Forensics Investigations:

Mobile phone forensics: mobile device characteristics, memory considerations, tools classification, flasher boxes, obstructed devices, forensics procedures: preservation, acquisition, examination and analysis, reporting; SIM Card Forensics.

Network Forensics: sources of network based evidences, procedure for applying network based forensics, digital evidence on internet, digital evidence on physical and data link layers, digital evidence at the network and transport layers.

Unit IV : Security Issues and Principles:

Risk Analysis: Terms and Definitions, Need, Methodology, Considerations and Approaches.

Security Models: IA-CMM,ISM3, SSE-CMM: Importance, Usage, Structure and Architecture, Process Areas; Security Engineering and its need.

Security Standards and frameworks: ISO 27001: Evolution, Organizational Context, ISMS Implementation in Organizations; COBIT: Principles, Structure and Objectives.

Security Methodologies: IAM, IEM, OCTAVE, OSSTMM,SIPES.

Laws for Information Security: Introduction to The Indian IT Act, IPR, Patent law, Copyright Law.

Unit V : Security Audit/Assurance:

Security Audits : Need in Organizations, Auditor's responsibility, Types, Approaches, Technology- Based Audits : Penetration Testing and Vulnerability Scanning; Phases, Budgeting for Security Audits.

Privacy : Organizational implications, Practices ,Policy, Audits: Framework and Approach, Standards, Phases, Process : Design, Risk Analysis, Planning, Conducting, Reporting.

Text and Reference books:

[1] Nina Godbole, Information Systems Security-Security Management, Metrics, Frameworks and Best Practices, Wiley, 2009.

[2] Digital Forensics and Cyber Crime; Ibrahim Baggili; Springer.

[3] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Massachusetts, Ed. Boston: Addision Wesley, 2001.

[4] Rick Ayers, Sam Brothers and Wayne Jansen : Guidelines on Mobile Device Forensics, NIST, 2014.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP4C1: Secure Wireless Networks	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:

- Provide students with enhance base of knowledge of wireless networking.
- Learn Security Issues in different wireless networks and mitigation techniques
- Develop a comprehensive knowledge of Tools and Techniques used in Management of wireless Networks
- Develop ability to carry out research in area of security in wireless Networks

COURSE CONTENT

Unit I : Foundation

Review of wireless communication Technologies : Cellular Networks, Wireless LAN, Prersonal Area Networks, Adhoc and Sensor Networks, Challenges in Adhoc and Sensor networks: Constrained Resources, Security, Mobility

Unit II :

Adaptability in Mobile computing, Mobility Management: Location Management Principles and Techniques, Data Dissemination and Management.

Unit III : Mobile and Wireless Security Issues, Approaches to security, Security in Wireless Personal Area Networks: Bluetooth Security Modes, Bluetooth Security Mechanisms, Authentication and Encryption in Bluetooth networks.

Unit IV :

Security in Wireless Local Area Networks: WEP, WPA, IEEE802.11i, Security in Metropolitan Area Networks: IEEE 802.16 and Security.

Unit V :

Security in Wide Area Networks: GSM Security, Four Generations of Wireless: 1G-4G, limitations and Security. Security in Ad hoc and Sensor networks.

Text and Reference books:

[1] Fundamentals of Mobile and Pervasive Computing, Frank Adelstein, S.K. Gupta, G. Richard
[2] III, L. Schwiebert, Mc Graw Hill, Ed.2005.
[3] Hacking Exposed : Mobile Secrets & Solutions, N.Bergman, M.Stanfield, J.Rose, J. Scambray.
[4] Building Secure Wireless Networks with 802.11, Jahanzeb Khan and Anis Khwaja, Wiley 2003.
[5] Ad Hoc Wireless Networks - Architectures and Protocols, C.Siva Ram Murthy and B.S.Manoj., Prentice Hall, 2004
[6] Technical Papers.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP3G2: Applied Cryptography	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**0**	**3**	**1**	**0**	**4**

Course Objective:
To impart the knowledge of encryption and decryption techniques and their applications in managing the security of data.

COURSE CONTENT

Unit I : Modular Arithmetic and Multiplicative Group
Modular Arithmetic for advanced cryptography, Multiplicative group of integers ,, order of an element in , generator of , extended Euclidean algorithm, Pohlig-Hellman and Pollard-Rho algorithm for computing DLP, Integer factorization problems, Pollard-Rho factoring algorithm.

Unit II : Tools for Symmetric key & Public key Cryptography
Shannon ciphers and perfect security, computational ciphers and semantic security, efficient adversaries and attack games, trapdoor function schemes, trapdoor function pair schemes, ElGamal cryptographic system, ElGamal digital signatures, fun applications.

.

Unit III : Block Ciphers and Their Attacks
Polynomial arithmetic, finite field GF(2^n), constructing block cipher in practice, sophisticated attacks on block ciphers, case study block cipher AES: AES structure, AES transformation functions, AES key expansions, AES Implementation, fun applications.

Unit IV : Cryptanalysis, IDS and Attacks
Intrusion detection system (IDS), cross site scripting attacks, SQL injection attacks, fault injection attacks, side channel attacks, algorithmic attacks.

Unit V : Asymmetric Key Cryptosystems
MD5 Message Digest Algorithm, Message authentic codes, Hash functions, Secure Hash Algorithms, Hash based message authentic code. Elliptical Curve Cryptography (ECC). Problems with the public key exchange.

Text and Reference books:

[1] Douglas R. Stinson;"Cryptography Theory and Practice"; Chapman & Hall/CRC
[2] Williams Stallings; "Cryptography & Network Security"; Pearson Education.
[3] Mathew Bishop; Introduction to computer Security; Addison-Wisley
[4] Atul Kahate; "Cryptography and Network Security"; Tata McGraw-Hill.

Devi Ahilya University, Indore, India Institute of Engineering & Technology				ME II Year Information Technology (Sp. Information Security) Semester- B			
Subject Code & Name	**Instructions Hours per Week**			**Credits**			
ISP4E1: Biometric Systems & Security	**L**	**T**	**P**	**L**	**T**	**P**	**Total**
Duration of Theory Paper: 3 Hours	**3**	**1**	**2**	**3**	**1**	**1**	**5**

Course Objective:
To study the concepts of various biological based information security systems.

COURSE CONTENT

Unit I : Overview of Biometrics
Definitions, biometric modalities, course outline, Basic applications: access control, e-commerce, forensics.

Unit II : Design of a Biometric System
Building blocks, Modes of operation, Fingerprint verification: Minutiae Based Fingerprint Matching, Non-minutiae Based Representations, Fingerprint Enhancement, and Fingerprint Classification. Face Recognition:- Introduction, Authentication vs. Identification, Challenges in Face recognition, Algorithms for face recognitions.
.

Unit III : Iris Recognition
Introduction, devices for capturing Iris, Iris representation schemes, Iris recognition algorithms. Biometrics based on hand geometry, signature, ear, palm, voice and DNA.

Unit IV : Multimodal Biometrics
Limitations of unimodal systems, multibiometric scenarios, levels of fusion, system design, score fusion techniques, score normalization, user-specific parameters, and soft biometrics.

Unit V : Case Study Presentations
Biometrics in Banking Industry, Biometrics in Computerized, Patient Records, Biometrics in Credit Cards, Biometrics in Mass Disaster Victim, Identification Forensic Odontology

Text and Reference books:

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar; “Handbook of Fingerprint Recognition”; Springer Verlag, 2003.
[2] A.K. Jain, R. Bolle, S. Pankanti (Eds.); “BIOMETRICS: Personal Identification in Networked Society”, Kluwer Academic Publishers, 1999.
[3] J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.); Biometric Systems: Technology, “Design and Performance Evaluation”; Springer, 2004.