

INDIAN SCHOOL OF ANTI HACKING
Maulana Abul Kalam Azad University of Technology West Bengal (MAKAUT WB)
[Formerly Known as WBUT]
B.Sc. in Digital Forensic
(Choice Based Credit System)

Course Structure:

B.Sc. in Digital Forensic	
Course Duration	3 Years (6 Semesters)
Course Credit	140

I. Core Courses (Credit94)

Year	Semester	Paper Code	Core Course Code	Paper Name
First	I	BSDF-101	C1	Fundamentals of Digital Systems
		BSDF-102	C2	Introduction to Programming
	II	BSDF-201	C3	Introduction to Digital Forensics & Cyber Laws
		BSDF-202	C4	Data Structures using C++
Second	III	BSDF-301	C5	Operating Systems and System Software
		BSDF-302	C6	Computer Networks and Network Security
		BSDF-303	C7	Biometric Security
	IV	BSDF-401	C8	Database Management Systems and Security
		BSDF-402	C9	Software Engineering
		BSDF-403	C10	Applied Cryptography
Third	V	BSDF-501	C11	Computer Forensics
		BSDF-502	C12	Preserving and Recovering Digital Evidence
	VI	BSDF-601	C13	Mobile Forensics and Wireless Security
		BSDF-602	C14	Malware Analysis

II. Generic Elective Courses (Credit 16, Semester- I to Semester -IV)

Year	Semester	Paper Code	General Elective GE Code	Paper Name
First	I	BSDFGE-103A	GE-1	Computer Organization
		BSDFGE-103B	GE-2	Discrete Mathematics 1
	II	BSDFGE-203A	GE-3	Data Communication
		BSDFGE-203B	GE-4	Discrete Mathematics 2
Second	III	BSDFGE-304A	GE-5	Microprocessors
		BSDFGE-304B	GE-6	Linux and Java Programming
	IV	BSDFGE-404A	GE-7	Forensic Science and Development in Society
		BSDFGE-404B	GE-8	Operations Research

* Students can earn the credits by choosing elective courses from MOOC's basket for this segment – MOOC's basket will be updated on every six months i.e. prior to start of every semester (odd and even).

** Credits will be transferred as per the scheduled guidelines.

*** MOOC's basket will be shared once it updated.

**** Maximum Credit Points can be transferred Upto 20 out of Total Credit Point 140 from MOOC's Courses.

III. Discipline Specific Elective (Credit 18, Semester V and VI)

Year	Semester	Paper Code	DSE Code	Paper Name
Third	V	BSDFDSE – 503A	DSE-1	Advance Digital Forensics
		BSDFDSE – 503B	DSE-2	Security Threats And Modelling
		BSDFDSE – 503C	DSE – 4	Advance Digital Forensic and Cyber Crime
	VI	BSDFDSE – 603A	DSE – 5	Crime Scene Investigation
		BSDFDSE – 603C	DSE – 7	Financial Offences
		BSDFDSE – 603C	DSE – 8	Dissertation in Semester – VI

IV. Skill Enhancement Courses (Credit 8 , Semester III andIV):

Year	Semester	Paper Code	SEC Code	Paper Name
Second	III	BSDFSEC– 305	SEC-1	Cyber Security
	IV	BSDFSEC– 405	SEC-2	Image Processing and Pattern Recognition

V. Ability Enhancement Compulsory Courses (Credit 4, Semester I,II)

Year	Semester	Paper Code	AECC Code	Paper Name
First	I + II	BSDFAECC-1	AECC-1	Environmental Science
		BSDFAECC-2	AECC-2	English Communication
The School / Department will have an option to take either of the two papers in a Semester (I or II), while the students have to appear in both the papers.				

Credit Distribution
MatrixDepartment of Digital
Forensics
B.Sc. in Digital Forensics

Semester – I

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-101	Fundamentals of Digital Systems	3	1	0	4
2	BSDF-102	Introduction to Programming	3	1	0	4
3	BSDF-103	Generic Elective	3	1	0	4
Total Credit (Theory)			9	3	0	12
Practical						
1	BSDF-191	Laboratory-1-Fundamentals of Digital Systems	0	0	4	2
2	BSDF-192	Laboratory-2-Introduction to Programming	0	0	4	2
Total Credit (Practical)			0	0	8	4
Compulsory Ability Enhancement Course						
1	BSDF-181	English Communication	2	0	0	2
Total Credit (Semester – I)			20	6	16	18

Semester – II

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-201	Introduction to Digital Forensics & Cyber Laws	3	1	0	4
2	BSDF-202	Data Structures using C++	3	1	0	4
3	BSDF-203	Generic Elective	3	1	0	4
Total Credit (Theory)			9	3	0	12
Practical						
1	BSDF-291	Laboratory – 3 – Introduction to Digital Forensics & Cyber Laws (Acts and Proceedings)	0	0	4	2
2	BSDF-292	Laboratory – 4 – Data Structures using C++	0	0	4	2
Total Credit (Practical)			0	0	8	4
Compulsory Ability Enhancement Course						
1	BSDF-281	Environmental Science	2	0	0	2
Total Credit (Semester – II)			20	6	16	18

Semester – III

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-301	Operating Systems and System Software	3	1	0	4
2	BSDF-302	Computer Networks and Network Security	3	1	0	4
3	BSDF – 303	Biometric Security	3	1	0	4
4	BSDF – 304	Generic Elective	3	1	0	4
5	BSDFSEC – 305	Cyber Security	3	1	0	4
Total Credit (Theory)			15	5	0	20
Practical						
1	BSDF-391	Laboratory – 5 – Computer Networks and Network Security	0	0	4	3
2	BSDF-392	Laboratory – 6 – Cyber Security	0	0	4	3
Total Credit (Practical)			0	0	8	6

Total Credit (Semester – III)	15	5	8	26
--------------------------------------	-----------	----------	----------	-----------

Semester – IV

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-401	Database Management Systems and Security	3	1	0	4
2	BSDF-402	Software Engineering	3	1	0	4
3	BSDF – 403	Applied Cryptography	3	1	0	4
4	BSDF – 404	Generic Elective	3	1	0	4
5	BSDFSEC – 405	Image Processing and Pattern Recognition	3	1	0	4
Total Credit (Theory)			15	5	0	20
Practical						
1	BSDF-491	Laboratory – 7 – Database Management Systems and Security	0	0	4	4
2	BSDF-492	Laboratory – 8 – Image Processing and Pattern Recognition	0	0	4	4
Total Credit (Practical)			0	0	8	8
Total Credit (Semester – IV)			15	5	8	28

Semester – V

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-501	Computer Forensics	3	1	0	4
2	BSDF-502	Preserving and Recovering Digital Evidence	3	1	0	4
3	BSDFDSE – 503	Discipline Specific Elective	3	1	0	4
4	BSDFDSE – 503	Discipline Specific Elective	3	1	0	4
Total Credit (Theory)			12	4	0	16
Practical						
1	BSDF-591	Laboratory – 9 – Computer Forensics	0	0	4	4
2	BSDF-592	Laboratory – 10 – Preserving and Recovering Digital Evidence	0	0	4	4
Total Credit (Practical)			0	0	8	8
Total Credit (Semester – V)			12	4	8	24

Semester – VI

Sl. No.	Paper Code	Paper Name	Credit			
			L	T	P	C
Theory						
1	BSDF-601	Mobile Forensics and Wireless Security	3	1	0	4
2	BSDF-602	Malware Analysis	3	1	0	4
3	BSDFDSE – 603	Discipline Specific Elective	3	1	0	4
4	BSDFDSE – 603D	Dissertation in Semester – VI	0	0	6	6
Total Credit (Theory)			9	3	6	18
Practical						
1	BSDF-691	Laboratory – 11 – Mobile Forensics and Wireless Security	0	0	4	4
2	BSDF-692	Laboratory – 12 – Malware Analysis	0	0	4	4
Total Credit (Practical)			0	0	8	8
Total Credit (Semester – VI)			18	6	28	26

Semester – I

Paper – I – FUNDAMENTALS OF DIGITAL SYSTEMS (BSDF – 101)

Module I:

Number Systems, Operations and Codes, Decimal Numbers, Binary Numbers, Decimal to Binary Conversion, Binary Arithmetic, 1's and 2's complement of binary numbers, Signed numbers, Arithmetic operations with signed numbers,

Hexadecimal numbers, Binary to hexadecimal conversion, Hexadecimal to binary conversion, Hexadecimal to decimal conversion, Decimal to Hexadecimal conversion, Hexadecimal addition and subtraction, Octal numbers, Octal to decimal conversion, Decimal to Octal conversion, Octal to binary conversion, Binary to Octal conversion, Binary coded decimal, 8421 BCD code, BCD addition, Digital codes- gray code, binary to gray code conversion, Alphanumeric codes, parity codes.

Module II:

Logic Gates, Logic Levels and Waveforms, Logic Levels and Digital waveforms, Logic Gates: AND, OR, NOT, XOR, XNOR, NAND (Definition, Symbols, Truth Tables and Operation). Universal Property of NAND and NOR gates. Logic gate operations with pulse waveforms.

Module III:

Boolean Algebra and Logic Simplifications. Boolean operations and expressions, Laws and rules of Boolean algebra, De-morgans theorems, Boolean analysis of logic circuits, simplification using Boolean algebra, standard forms of Boolean expression, Boolean expressions and truth tables. The Karnaugh Map, Karnaugh SOP minimization, Karnaugh POS minimization, Five variable Karnaugh maps.

Module IV:

Combinational Logic and its functions, Basic combinational Logic circuits, Implementing combinational logic, combinational logic using NAND and NOR gates, Basic overview of logic functions, Basic adders, parallel binary adders, comparators, decoders, encoders, code converters, multiplexers, demultiplexers, parity generators/ checkers.

Module V:

Sequential Circuits, Latches, RS flip flop using NAND/ NOR gates, Clocked RS, D, JK and T flip flops, Edge triggered flip flops, Master slave flip flops, Asynchronous counter operation, Synchronous counter operations, Up/ Down Synchronous counter, Design of synchronous counters. Basic shift register functions. Serial in-Parallel out shift registers, Parallel in -Serial out shift registers, Serial in- Serial out shift registers, Parallel in Parallel out shift registers.

References

Reference Books:

1. 1. Floyd and Jain- Digital Fundamentals, Eighth Edition, Pearson Education.
2. 2 .A P Malvino and D P Leach - Digital Principles and Applications, Fourth edition, Tata McGraw Hill Publishers, co Ltd.

Paper-II-Introduction to Programming(BSDF-102)

Module I

Introduction to programming, Classification of computer languages, Language translators (Assembler, Compiler, Interpreter), Linker, Characteristics of a good programming language, Factors for selecting a language, Subprogram, Purpose of program planning, Algorithm, Flowchart, Pseudo code, Control structures (sequence, selection, Iteration), Testing and debugging. Procedure Oriented Programming- Object Oriented Programming- A simple C++ program- Structure of C++ program-Tokens- Data types- variables- Symbolic constants- Reference by variables-Operators in C++- Operator precedence- Control structures- Arrays.

Module II

Classes and Objects: Function in C++ - The main function, Function prototyping- Call by value- Call by reference- Return by reference. Basic concepts of object-oriented programming- Benefits of OOP- Applications of OOP. Specifying a class- Defining member functions-Private member functions- Arrays within a class - Memory allocation for objects-Static data members -Static member functions - Arrays of objects -Friendly functions.

Module III

Constructors- Default constructor-Parameterized constructor-Copy constructor- Multiple constructors-Constructors with default arguments- Dynamic constructor-Destructors- Operator overloading- Unary and Binary operator overloading- Overloading using friends- Rules for overloading- Type conversion.

Module IV

Inheritance- Defining derived classes-Visibility modes-Single, Multilevel, Multiple, Hierarchical and Hybrid inheritance- Virtual base classes- Abstract classes- Constructors in derived classes.

Module V

Pointers- Pointers to objects- this pointer-Pointers to derived classes- Virtual functions- Pure virtual functions-Opening and closing a file- File opening modes- File pointers and their manipulations- Sequential input and output operations.

Reference Books:

1. Object oriented Programming with ANSI & Turbo C++,Ashok N. Kamthane,First Edition, 2011, Pearson India.
2. Computer Fundamentals,P K Sinha&PritiSinha, Reprint 2018, BPB Publications.
3. Object Oriented Programming with C++,E. Balagurusamy , Fifth edition, Tata McGraw Education Hill, 2011.
4. Programming in C,AshokKamthane Third Edition, 2015, Pearson Education.
5. Object Oriented Programming in Turbo C++,Robert Lafore,1991, First Edition, Galgotia Publications.
6. Programming with C++,DRavichandran, Second edition, 2002, Tata McGraw- Hill.

Semester – II

Paper–I–Introduction to Digital Forensics & Cyber Laws(BSDF–201)

Module I

Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases. Analyzing malicious software. Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems

Module II

Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems ,Router Forensics. Cyber forensics tools and case studies. Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.

Module III

Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Investigating Web attacks, Investigating network Traffic ,Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events.

Module IV

Basic of law, Understanding cyber space, Defining cyber law, Scope and jurisprudence , Concept of jurisprudence, Overview of Indian legal system, Introduction to IT Act 2000, Amendment in IT Act.

Module V

Cyber Crimes – Types of cyber crimes –against individuals institution, and states-various offenses and punishments, digital signature-concepts of public key and private key, certification authorities and their role, creation and authentication of digital signature. E-contracting –salient features of E-contracts, formation of E-contracts and types, E-governance, E-governance models, E-commerce-salient features and advantages.

Reference Books:

1. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition,John R. Vacca, Charles River Media,2005
2. Cyber Forensics - Concepts and Approaches, Ravi Kumar &B Jain,2006, icfaiuniversitypress
3. Understanding Cryptography: A Textbook for Students and Practitioners,ChristofPaar, Jan Pelzl, 2010, Second Edition,Springer's.
4. Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri,First edition, 2009
5. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press

Series: Computer Forensics),2010

6. "Internet Complete Reference, Harley Hahn, second Edition, 1996, Osborne/McGraw- Hill
7. Internet and Web design, , Ramesh Bangia Firewall Media, (An imprint of Lakshmi Publications Pvt. Ltd.). Second Edition 2006.
8. Cyber Law Crimes, Barkhs and U. Rama Mohan, Third Edition ,2017,Asia LawHouse
9. Cyber Laws Simplified,ViveekSood, Fourth reprint 2008,McGrawHill.

Paper-II-Data Structures using C++(BSDF-202)

Module I

Introduction to Data Structures, Basic Terminology, Data Structure Operations; Algorithm: Definition, Algorithm Analysis, Complexity, Asymptotic Notation, Recursion. Array: Introduction, Linear Arrays, Representation of Linear Arrays in Memory, operations; Multidimensional Arrays.

Module II

Stack: Introduction, Array Representation and Basic Operations; Implementation of Stacks. Application of Stacks, Evaluating Arithmetic Expression using Stacks, Infix to Postfix Notation, Evaluating a Postfix Notation.

Module III

Queue: Introduction, Implementation of Queue, Priority Queue, Dequeue, Linked List: Introduction, Representation of Linked List, operations in Linked List, Doubly and Circular Linked List.

Module IV

Trees - Introduction, Binary Trees, Representation, Traversing and its Algorithms, AVL tree.

Module V

Sorting: Bubble sort, Insertion sort, Selection sort, Heap sort, Quick sort, Merge sort; Comparison of sorting algorithms. Searching: Linear Search, Binary Search; Comparison of searching algorithms.

Reference Books:

1. Schaum's Outline Series: Theory and Problems of Data Structures-Seymour Lipschutz, 1986, McGraw-Hill.
2. Data Structures and Algorithms in C++, Goodrich Michael T, Second edition, 2016, Wiley.
3. Data structures and Algorithm Analysis in C++, Mark allen Weiss, Third edition, 2007, Pearson Education India.
4. Data Structures, Seymour Lipschutz, Revised First edition, 2014, McGraw Hill Education.

SEMESTER – III

Paper – I – Operating Systems and System Software (BSDF – 301)

Module I

Definition- Functions- OS as Resource Manager, Types – Structure- Concept of Batch Processing, Multi-programming, Multi-user systems and Real-time systems, POST Bootstrapping – Kernel

Module II

Process management: process concept, process scheduling, operations on processes, cooperating processes, interprocess communication, communication in client server systems, threads, overview, multithreading models, CPU scheduling, scheduling criteria, CPU scheduling algorithms, process synchronization, critical-section problem semaphores, deadlocks, prevention, avoidance and detection.

Module III

Storage Management: memory management, contiguous memory allocation, paging, segmentation, segmentation with paging, virtual memory, demand paging, page replacement. I/O hardware ,I/O Software , Disks – Disk Scheduling . File organization ,File system implementation , allocation methods, Security , Protection mechanism

Module IV

General concepts - system software and application software, Assemblers- Design of assembler, Macros and Macroprocessor, Macro definitions& Instructions, Features of macro facility, Nested macros calls.

Module V

Loading, Linking & Relocating- Loading& Linking Schemes- Relocatability of Programs, Concepts of Binders, Linking Loaders, Overlays, Dynamic Binders, Design of an absolute loader. Compilers – Different phases of compilers

Reference Books:

1. Operating System Concepts – Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, 8th Revised edition edition, 2008,Wiley.
2. System programming &Operating Systems D.M. Dhammdhere, Second revised edition, reprint 2009. Tata McGrawHill
3. Operating System- Manick& Donovan, reprint 2008,McGrawHill
4. Operating system –H M Deitel, 2007, PearsonEducation
5. System Programming - John J Donovan , 2017, Tata McGraw Hill

Paper-II-Computer Networks and Network Security(BSDF-302)

Module I

Introduction: - Types of Computer Networks, Reference Models - ISO-OSI Reference Model, TCP/IP Reference Model.

Protocol Hierarchies Network layer: Routing Algorithm , ARP,RARP-Transport Layer: Elements of transport protocols, UDP, Segment Structure, TCP ,Service model, TCP Protocol, Application Layer: HTTP, DNS.

Module II

Computer Security Concepts, the OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. Access Control Models, Chinese Wall, Clark-Wilson, Bell-LaPadula, Non Interference and Role Base Model.

Module III

Symmetric Encryption Principles, Symmetric Block Encryption Algorithms. Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures. Key Distribution and User Authentication: Symmetric Key Distribution Using Symmetric Encryption, Kerberos, Key Distribution Using Asymmetric Encryption,X.509 Certificates, Public-Key Infrastructure.

Module IV

Transport-Level Security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, Transport Layer Security, HTTPS, Secure Shell (SSH). IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange.

Module V

Electronic Mail Security: Pretty Good Privacy, S/MIME. Intruders: Intruders, Intrusion Detection, Password Management. Firewalls: The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations.

Reference Books:

1. Network security essentials, William Stallings, fourth edition, 2011 Pearson Education
Computer
2. Networks,Andrew S. Tanenbaum, fifth Edition, 2013, Pearson Education India.
3. Data communications and networking, Behrouz A. Forouzan, 2017,McGraw Hill Education.

Paper – III – Biometric Security (BSDF – 303)

Module I

Biometric fundamentals and standards: Definition, Biometrics versus traditional techniques, Characteristics, Key biometric processes: Verification - Identification - Biometric matching, Performance measures in biometric systems, assessing the privacy risks of biometrics - Designing privacy sympathetic biometric systems, Different biometric standards, and Application properties.

Module II

Physiological Biometric Technologies: Fingerprints ,Technical description, characteristics , Competing technologies ,strengths, weaknesses ,deployment ,Facial scan , Technical description ,characteristics ,weaknesses-deployment ,Iris scan ,Technical description , characteristics, strengths ,weaknesses ,deployment

Module III

Retina vascular pattern, Technical description, characteristics, strengths, weaknesses, Deployment, Hand scan, Technical description, characteristics, strengths, weaknesses deployment, DNA biometrics. Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics.

Module IV

Signature and handwriting technology, Technical description, classification, keyboard / keystroke dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses, deployment.

Module V

Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Reference Books:

1. Handbook of Biometrics, Anil K Jain, Patrick Flynn and Arun A Ross, 2010, Springer, USA.
2. Biometric Technologies and Verification Systems, John R Vacca, 2009, Elsevier, USA
2. Biometrics-Identity verification in a network, Samir Nanavathi, Michel Thieme, and Raj Nanavathi, 1st Edition, 2002, Wiley Eastern.
3. Implementing Biometric Security, John Chirillo and Scott Blaul, 1st Edition, 2005, Wiley Eastern Publication..
4. Biometrics for Network Security, John Berger, 1st Edition, 2004, Prentice Hall.

Semester – IV

Paper-I-Database Management Systems and Security(BSDF-401)

Module I

Introduction: Characteristics of the Database approach, Problems with file system data management, Data models, Schemas and instances, Database System Architecture, Data Abstraction, Data Independence, Data Definitions and Data Manipulation Languages.

Data models, Entity Relationship (ER), Mapping ER Model to Relational Mode, Weak and strong entity, Enhanced Entity Relationship (EER) and object modeling. specialization and generalization, Network. Relational and Object Oriented Data Models, Integrity Constraints and Data Manipulation Operations.

Module II

Physical Data organization, Hashed files, Indexed files, B- Trees, sequential Organization files. The relational Data model concepts, Relational model constraints, Relational algebra, Tuple relational calculus, Domain relational calculus, SQL.

Database design, Functional dependencies, Basic definitions, Trivial and non trivial dependencies, Closure of a set of dependencies, closure of a set of attributes, Irreducible set of dependencies, Non loss decomposition and functional dependencies First, Second and Third Normal forms, Boyce –Codd Normal forms.

Module III

Introduction- Introduction to Databases Security Problems in Databases .Database Integrity and Security Concepts, Domain constraints, Referential Integrity .Introduction to database security concepts, Methods for database security, Discretionary access control method, Mandatory access control and role base access control for multilevel security. Use of views in security enforcement. Overview of encryption technique for security. Statistical db security.

Module IV

Crash Recovery, Failure classification, Recovery concepts, Log base recovery techniques (Deferred and Immediate update), Checkpoints, Recovery with concurrent transactions (Rollback, checkpoints, commit), Database backup and recovery from catastrophic failure. Shadow paging.

Security Models -2 Bell and LaPadula's Model Biba's Model, Dion's Model, The Lattice Model for the Flow Control.

Module V

Security Mechanisms: User Identification/Authentication Memory Protection, Resource Protection, Control Flow Mechanisms Isolation Security .Secure DBMS Design Security

A Model for the Protection of Object Oriented Systems, SORION Model for the Protection of Object-Oriented Databases

Reference Books:

1. Database system concepts, Silberschatz, H.F Korth, and S Sudarsan,, Fourth Edition, 2002 Tata McGraw Hill.
2. Database Security and Auditing, Hassan A. Afyouni, India Edition, 2009 cengage Learning.
3. Database Security, Silvana Castano, Second edition 1994, Pearson Education.
4. Fundamentals of Database Systems, Elmasri and Navathe, 3/e, 2003, Pearson Education,
5. Database systems- Design Implementation and Management, Peter Rob, Carlos Coronel, 10 edition, 2012, Course Technology

Paper-II-Software Engineering(BSDF-402)

Module I

Introduction to Software Engineering, Definition, Program Vs Software, and Software process, Software Characteristics, Brief introduction about product and process, Software process and product matrices.

Module II

Software life cycle models, Definition, Waterfall model, Increment process models, Evolutionary process models, Selection of a life cycle model.

Module III

Software Requirement Analysis and Specification Requirements Engineering type of requirements, Feasibility Studies, Requirement Elicitation, Various steps for requirement analysis, Requirement documentation, Requirement validation. Project planning-Size estimation, cost estimation, the constructive cost model (COCOMO)

Module IV

Design concept and principles:architectural designs, user interface design

Module V

Software Testing What is testing?, Test, Test case and Test Suit, Verification and Validation, Alpha, beta and acceptance testing, functional testing, Levels of testing ,types of s/w test ,black box testing ,Unit testing, integration testing, validation testing, testing boundary conditions, structural testing , regression testing, system testing and debugging.

Reference Books:

1. Software Engineering ,Roger S . Pressman, Sixth edition, 2004, TataMcgraw - Hill InternationalEdition.
2. Software Engineering Programs Documentation Operating procedures, K.K. Aggarwal&Yogesh Singh,2003, New Age InternationalPublishers
3. Software engineering,IanSommerville, Sixth edition,2001,Pearson educationAsia.

Paper – III – Applied Cryptography (BSDF – 403)

Module I

Foundation, Terminology, Substitution Cipher and Transposition Cipher, Simple XOR One Time Pads, Computer Algorithms, Large Numbers, Cryptographic Protocols, Communication using Symmetric Cryptography, One Way Functions-One Way Hash Function Communications using Public Key Cryptography, Digital Signatures-Digital Signature with Encryption, Random and Pseudo Random Sequence Generation.

Module II

Basic Protocols-Key Exchange, Authentication, Authentication and Key Exchange, Formal Analysis of Authentication and Key Exchange Protocols-Multiple Key Public Key Cryptography, Secret Splitting-Secret Sharing. Intermediate Protocols, Timestamp Services- Subliminal Channel, Undeniable Digital Signature- Proxy Signature, Group Signature

Module III

Advanced Protocols, Zero knowledge proofs, Zero knowledge proofs of identity, Blind Signature, Identity based Public key cryptography-Digital Certified Mail. Esoteric Protocol ,Secure Elections, Secure Multiparty Computation, Anonymous Multiparty Computation- Anonymous Message Broadcast, Digital Cash

Module IV

Cryptographic Techniques, Key length, Key Management, Public Key Cryptography Versus Symmetric Cryptography, Encrypting communication Channel, Encrypting Data for storage- Hardware vs software Encryption. Cryptographic Algorithm, Information Theory, Data Encryption Standard (DES), IDEA, Blowfish.

Module V

One way Hash Function- N Hash- MD4- MD5-MD2- Secure Hash Algorithm(SHA)- Public Key algorithms, Knapsack Algorithm, RSA- Public Key Digital Signature Algorithms- Digital Signature Algorithm(DSA)- DSA Variants- Gost Digital Signature Algorithm, Key Exchange Algorithm- Diffie Hellman – Station to Station Protocol, Encrypted Key Exchange

Reference Books:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.
2. Cryptography and Network Security: Principles and Practice, William Stallings, sixth edition, 2013, Pearson.

Semester – V

Paper-I-Computer Forensics(BSDF-501)

Module I

Introduction, Investigating Computer Crime, Steps to Prepare for a Computer Forensics Investigation, Computer Forensics Investigation Methodology

Module II

Data Acquisition and Duplication Concepts, Data Acquisition Types, Validation Methods

Module III

Volatile Memory Forensics, Defeating Anti forensic technique (Steganography, Password breaking, decryption), Deleted File Recovery

Module IV

Operating System Forensics, Windows Forensics, Linux Forensics, Metadata Extraction

Module V

Event Log Analysis, Registry Analysis, Network Forensics, Investigating EMail Crimes, Report Writing and Presentation

Reference Books:

1. Insider Computer Fraud, Kenneth C. Brancik, 2008, Auerbach Publications Taylor & Francis Group,
2. Ethical Hacking, Ankit Fadia, Second edition, 2006, Macmillan India Ltd.

Paper-II-Preserving and Recovering Digital Evidence(BSDF-502)

Module I

Digital Investigation: Digital evidence and computer crime ,history and terminals of computer crime investigation ,technology and law ,the investigate process ,investigate reconstruction ,modus operandi, motive and technology ,digital evidence in the court room.

Module II

Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems ,forensic examination of unix systems ,forensic examination of macintosh systems, forensic examination of handheld devices.

Module III

Networks: Networks basics for digital investigators, applying forensic science to networks,digital evidence on physical and datalink layers ,digital evidence on network and transport layers ,digital evidence on the internet.

Module IV

Investigating Computer Crime: Investigating computer intrusions ,investigatingcyberstalking,digital evidence as alibi.

Module V

Guidelines: Handling the digital crime scene – digital evidence examination guidelines.

Reference Books:

1. Digital Evidence and Computer Crime Forensic science, Computers and Internet, EoghanCasey,Second Edition, 2011 ,Elsevier AcademicPress.
2. A Electronic Discovery and Digital Evidence in a Nut Shell-Daniel J Capra,Shira A scheindlin,-Third Edition, 2009 The Sedona Conerence-AcademicPress.
3. The Best Damn Cybercrime and Digital Forensics Book Perio,Jack Wiles, Anthony Reyes , Jesse Varsalone,2007 SyngressPublishing.
4. Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet.Casey, Eoghan, 2000 , Cambridge UniversityPress
5. Computer Forensics Computer Crime Scene Investigation,Vacca, John R. ,2002,Charles River Media.

SEMESTER – VI

Paper-I–Mobile Forensics and Wireless Security(BSDF–601)

Module I

Wireless Fundamentals: Wireless Hardware, Wireless Network Protocols, Wireless Programming WEP Security. Wireless Cellular Technologies, concepts, Wireless reality, Security essentials, Information classification standards, Wireless Threats: Cracking WEP , Hacking Techniques, Wireless Attacks, Airborne Viruses.

Module II

Standards and Policy Solutions , Network Solutions , Software Solutions , Physical Hardware Security, Wireless Security , Securing WLAN , Virtual Private Networks , Intrusion Detection System , Wireless Public Key infrastructure. Tools, Auditing tools, Pocket PC hacking, wireless hack walkthrough.

Module III

Security Principles, Authentication, Access control and Authorization, Non-repudiation, privacy and Confidentiality, Integrity and Auditing, Security analysis process. Privacy in Wireless World, Legislation and Policy, Identify targets and roles analysis, Attacks and vulnerabilities , Analyze mitigations and protection.

Module IV

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.

Module V

Global Mobile Satellite Systems; case studies of the IRIDIUM and GLOBALSTAR systems. Wireless Enterprise Networks: Introduction to Virtual Networks, Blue tooth technology, Blue tooth Protocols. Server-side programming in Java, Pervasive web application architecture, Device independent example application

Reference Books:

1. Wireless Security Essentials: Defending Mobile from Data Piracy, Russel Dean Vines , First Edition, 2002, John Wiley & Sons,.
2. Maximum Wireless Security, Cyrus, Peikari and Seth Fogie, 2002, SAMSPublishing.
3. Wireless and Mobile Networks Architectures, Yi-Bing Lin and Imrich Chlamtac, 2001, John Wiley & Sons.
4. Mobile and Personal Communication systems and services, Raj Pandya, 2001, Prentice Hall of India..
5. Wireless Security and Privacy- Best Practices and Design Techniques, Tara M. Swaminathan and Charles R. Eldon, 2002, AddisonWesley.

Paper-II–Malware Analysis(BSDF–602)

Module I:

World of Malwares, What is Malware?,Kinds of Malware, Why Malware is being created?, Various Terminology about Malware

Module II

Malware Analysis Lab Setup, Creating your own Virtual World, A Copy of Windows XP / 7, Tools for analysis of the Windows Malware, Prohibition on Connection Between Virtual System and Host System

Module III

Basic Static Analysis of Malware, Anti-Virus Scanning, Hashing: Fingerprint of Malware
Detecting Packers, Analysing PE file Headers and Sections, Module 12: Basic Dynamic Analysis of Malware, Running Malware using Sandboxie, Analysing the Process of Malware, Monitoring, Registry Changes, Network Traffic Analysis

Reference Books:

1. M.Y. Iscan and S.R. Loth, The scope of forensic anthropology in, Introduction to Forensic Sciences, 2nd Ed., W.G. Eckert (Ed.), CRC Press, Boca Raton(1997).
2. D. Ubelaker and H. Scammell, Bones, M. Evans & Co., New York(2000).
3. S.Rhine, Bone Voyage: A Journey in Forensic Anthropology, University of Mexico Press, Mexico(1998)

