SHIVAJI UNIVERSITY, KOLHAPUR - 416004,
MAHARASHTRA
PHONE:EPABX-2609000, www.unishivaji.ac.in, bos@unishivaji.ac.in
शिवाजी विद्यापीठ, कोल्हापूर -४१६००४,महाराष्ट्र
दूरध्वनी-ईपीएबीएक्स -२६०९०००, अभ्यासमंडळे विभाग दुरध्वनी ०२३१—२६०९०९४
०२३१—२६०९४८७

Estd. 1962
"A++" Accredited by
NAAC (2021)
With CGPA 3.52

Ref.No.SU/BOS/Science/249 **Date: 08/07/2026**

The Head /Director/Co-ordinator
All Concerned Department (Science)
Shivaji University, Kolhapur.

Subject: Regarding Structure and syllabus of **B.Sc. Part I** under the Faculty of Science and Technology as per **Apprenticeship Embedded Degree Programme (AEDP).**

Sir/Madam,

With reference to the subject mentioned above, I am directed to inform you that the university authorities have accepted and granted approval to the structure and syllabi, nature of question paper of **B.Sc. Part I** under the Faculty of Science & Technology as per **Apprenticeship Embedded Degree Programme (AEDP).**

B.Sc. Part-I (Sem. I & II) as per AEDP			
1.	Cyber Security & Digital Forensics	3.	Biochemistry
2.	Digital Marketing and AI	4.	Biotechnology

This structure and syllabi shall be implemented from the academic year 2026- 2027 onwards. A soft copy containing structure and syllabus is attached herewith and it is also available on university website **www.unishivaji.ac.in>Syllabus>Syllabus as per NEP2020.** This programme is introduce subject to approval of university authority for converted.

You are, therefore, requested to bring this to the notice of all students and teachers concerned.

Thanking you,

Yours faithfully,

Dy Registrar

Encl: as above
for information and necessary action

Copy to:

1	Dean, Faculty of Science & Technology	7	Appointment A & B Section
2	Director, Board of Examinations and Evaluation	8	I.T.Cell /Computer Centre
3	Chairman, Respective Board of Studies	9	Eligibility Section
4	B.Sc.-M.Sc. Exam Section	10	Affiliation (T.1) Section
5	Internal Quality Assurance Cell (IQAC Cell)	11	Affiliation (T.2) Section
6	Est PG Section	12	P.G. Seminar Section

SHIVAJI UNIVERSITY, KOLHAPUR

NAAC A++ Grade with CGPA 3.52

Multiple Entry and Multiple Exit Option (NEP-2020)

Syllabus for

B.Sc. Cyber Security & Digital Forensics

(Apprenticeship Embedded Degree Programmes)

B.Sc. (CS & DF) (AEDP)

(Under Faculty of Science and Technology)

PART- I SEMESTER –I & II

(Syllabus to be implemented from Academic year 2026 - 2027)

B.Sc. Cyber Security & Digital Forensics (AEDP)

1. Title: B.Sc. Cyber Security & Digital Forensics (AEDP)
2. Year of implementation: Syllabus will be implemented from June 2026 onwards
3. Duration: B.Sc. Cyber Security & Digital Forensics (AEDP) is Three years (6 semesters).
4. Pattern: Pattern of examination will be semester

Shivaji University, Kolhapur

B.Sc. Cyber Security & Digital Forensics (CS & DF)

(AEDP)

(Under Faculty of Science and Technology)

Program Outcomes

Upon successful completion of the **B.Sc. Cyber Security & Digital Forensics (CSDF)** programme, the student should have met the following outcomes:

1. Apply skills and concepts of Computer Science to understand, design, and develop computing solutions for real-world problems.
2. Ability to design, develop, and implement secure computing solutions using appropriate tools, technologies, and methodologies.
3. Apply mathematical, statistical, and analytical techniques to solve problems related to computing, cyber security, and digital investigations.
4. Apply Cyber Security and Digital Forensics principles, tools, and techniques to protect digital assets and investigate cyber incidents.
5. Recognize the importance of innovation and develop critical thinking and research aptitude to address emerging challenges in Cyber Security and Digital Forensics.
6. Recognize social, professional, legal, ethical, and cultural values and issues involved in the use of information technology, cyber security, and digital investigations.
7. Be self-motivated and enhance self-learning capabilities to adapt to emerging technologies and evolving cyber threats.

Program Specific Outcome (PSO)

1. An ability to enhance the application of Cyber Security and Digital Forensics knowledge in diverse domains.
2. Develop skills to identify cyber threats, vulnerabilities, and security risks in computing environments.
3. Focuses on preparing students for roles in Cyber Security, Information Security, Digital Forensics, and the IT industry.
4. Develop programming skills, networking skills, database skills, and security analysis skills using modern tools and technologies.

5. Information about various cyber security tools, forensic tools, and the latest developments in information security and digital investigation systems is provided.
6. Ability to identify, formulate, analyze, and solve cyber security and digital forensic problems using appropriate techniques and methodologies.
7. Take up self-employment opportunities in cyber security consulting, digital investigation services, and related technology sectors.
8. To pursue higher education, professional certifications, research, and careers in Cyber Security, Digital Forensics, Information Security, and related fields.
9. The student will be able to know various issues, challenges, and the latest trends in Cyber Security and Digital Forensics and thereby innovate new ideas and solutions to existing problems.

Programme Educational Objectives (PEOs)

The B.Sc. Cyber Security & Digital Forensics (CSDF) programme aims to:

1. Develop competent professionals with strong foundations in Cyber Security, Digital Forensics, Computing, and Information Security to address real-world security challenges.
2. Promote innovation, critical thinking, problem-solving abilities, and research aptitude for developing effective solutions in Cyber Security and Digital Forensics.
3. Encourage lifelong learning, professional growth, ethical practices, and adaptability to emerging technologies and evolving cyber threats.

1. Introduction

The B.Sc. Cyber Security & Digital Forensics (CSDF) programme is designed to provide students with the knowledge, skills, and abilities required to meet the growing demands of the Cyber Security and Digital Forensics industry. The programme focuses on developing a strong foundation in Computing, Cyber Security, Digital Forensics, Programming, Networking, Database Systems, and Information Security.

Beginning with the fundamental concepts of Computing and Cyber Security, the programme enables students to understand and apply security principles, digital investigation techniques, and emerging technologies through effective and practical modes of learning. The curriculum is designed to equip students with the competencies required to protect digital assets, identify and mitigate cyber threats, investigate cyber incidents, and analyze digital evidence.

The B.Sc. Cyber Security & Digital Forensics programme aims to prepare skilled professionals capable of addressing contemporary cyber security challenges and contributing to secure digital environments. The programme also encourages innovation, ethical practices, problem-solving abilities, and lifelong learning to help students adapt to evolving technologies and emerging cyber threats while pursuing careers in Cyber Security, Digital Forensics, Information Security, Digital Investigation, Security Operations, and related domains.

2. Multiple Entry and Multiple Exit Option (NEP-2020):

- After successful completion of First year of B.Sc. CS & DF Student can exit with under graduate certificate in Cyber Security & Digital Forensics.
- After successful completion of Second year of B.Sc. CS & DF Student can exit with under graduate Diploma in Cyber Security & Digital Forensics.
- After successful completion of Third year of B.Sc. CS & DF Student can exit with B.Sc. CS & DF degree programme.

3. Medium of Instruction:

The medium of instruction will be English only

4. Admission Procedure

To be eligible for admission to the B.Sc. CS & DF a candidate must have:

HSC (Std. XII) (Science or Commerce) or equivalent (Science/Commerce) through the Maharashtra Board or any recognized Board.

OR

Must have passed HSC (Std. XII) vocational subjects conducted by Maharashtra State Board of Secondary & Higher Secondary Education

OR

MCVC (Engineering Technology Group) passed.

OR

Any 3 year Diploma after SSC

5. Course Structure:

Lectures and Practical should be conducted as per the scheme of lectures and practicals indicated in the course structure.

6. Teaching and Practical Scheme

a) Each contact session for teaching 60 minutes each.

b) One Practical Batch should be of 30 students.

c) Practical evaluation should be conducted after the commencement of the University examination.

7. Project Work

a. Project work may be done individually or in groups in case of bigger projects. However, if the project is done in groups, each student must be given responsibility for a distinct module, and care should be taken to ensure that the progress of individual modules is independent of others.
b. Students should take guidance from the assigned guide and prepare a Project Report on "Project Work" in two copies to be submitted to the Head of the Department.
c. The project report should contain an Introduction to the Project, which should clearly explain the project scope in detail. Appropriate diagrams, system architecture, database designs, network architecture diagrams, security frameworks, workflow diagrams, digital forensic methodologies, and a list of outputs/reports generated should be included wherever applicable.
d. The Project Work should be of such a nature that it could prove useful or should be relevant from the Cyber Security, Digital Forensics, commercial, industrial, or societal perspective.
e. The project report will be duly assessed by the assigned guide and internal marks will be communicated by the Director of the Institute/Head of the Department.
f. The project report should be prepared in a format prescribed by the University, which also specifies the contents and methods of presentation. IEEE Computer Society templates are recommended in this regard.
g. The external viva shall be conducted by a panel of minimum two examiners, out of which one will be an external examiner and the other will be an internal examiner.

8. Assessment

a) The project will be evaluated by the university appointed examiners both internal as well as external.
b) The final practical examination will be conducted by the university appointed examiners both internal as well as external at the end of semester for each lab course and marks will be submitted to the university by the panel.

c) The practical examination will be conducted semester wise in order to maintain the relevance of the respective theory course with laboratory course.

d) The final examinations shall be conducted at the end of the semester.

Nature of question paper:

Internal Examination

Year	Semester	Activity	Marks (2 Credits)
1	I & II	1. Home Assignment 2. Quiz 3. Presentation / Demonstration 4. Midterm Test	5 5 5 5
Note:1.Midterm Test shall be conducted after completion of each unit			

Nature of question paper is as follows for University end semester examination

❖ **Theory Examination:**

Each paper will carry 30 Marks

1. Question No.1 is compulsory and is of multiple choice questions. There will be 6 multiple choice questions each carrying 1 mark
2. Question No.2 will have 3 questions out of which 2 questions need to be solved. Each carries 6 Marks
3. Question No.3 will have 6 questions out of which 4 questions need to be solved. Each carries 3 Marks

Practical Examination:

1 Each paper carries 30 Marks

2 Duration of Practical Examination: 2 Hrs

3 Nature of Question paper: There will be 3 questions out of which any 2 questions to be attempted and each question carries 15 Marks.

4 Internal Marks: 20(Journal :10 Marks, Internal Viva:10 Marks)

5 Practical evaluation should be conducted after the commencement of University examination by External examination.

6 Theory/Practical Exams of Open Elective will be conducted by Internal Evaluator.

9. Standard of Passing:

i) Minimum 40% marks in each subject. There shall be separate passing for theory and practical.

ii) Admission to B.Sc. Cyber Security & Digital Forensics (CS & DF) Part II is allowed even if the students fails in 20 subjects of First year B.Sc. Cyber Security & Digital Forensics (CS & DF)

iii) Admission to B.Sc. Cyber Security & Digital Forensics (CS & DF) part III is allowed even if the students fail in 20 subjects of B.Sc. Cyber Security & Digital Forensics (CS & DF) Part II. But no student is allowed to take admission to third year of B.Sc. Cyber Security & Digital Forensics (CS & DF) unless they clear all the papers of first year.

1. **Board of Paper Setters /Examiners:**

   For each Semester end examination there will be a board of Paper setters and examiners for every course. While appointing paper setter /examiners, care should be taken to see that there is at least one person specialized in each unit of the course.

2. **Credit system implementation:**

   As per the University norms

3. **Clarification of Syllabus:**

   The syllabus committee should meet at least once in a year to study and clarify any difficulties from the Institutes.

4. **Revision of Syllabus:**

   As the computer technology experience rapid rate of obsolescence of knowledge, revision of the syllabus should be considered every two/three years.

5. **Award of Class:**

   There will be numerical marking on each question. At the time of declaration of the result the marks obtained by the candidate is converted into grade point as shown below;

Grading: Shivaji University has introduced a Seven-point grading system as follows

Sr. No.	Marks Range out of 50	Grade Point	Letter grade
1.	40-50	10	O: Outstanding
2.	35-39	9	A+:Excellent
3.	30-34	8	A:Very Good
4.	28-29	7	B+:Good
5.	25-27	6	B: Above Average
6.	23-24	5	C:Average
7.	20-22	4	P:Pass
8.	0-19	0	F:Fail
9.	Absent	0	Ab: Absent

Multiple Entry and Multiple Exit Option (NEP-2020)

B.Sc. Cyber Security & Digital Forensics (AEDP)

Programme Structure

B.Sc. Part - I (Level-4.5)

Part – I Semester – I

SEMESTER-I (Duration-Six Month)								
Sr. No.	Course Code	**Teaching Scheme**			**Examination Scheme**			
		Theory and Practical			University Assessment(UA)		Internal Assessment (IA)	
		Lectures (Per week)	Hours (Per week)	Credit	Maximum Marks	Minimum Marks	Maximum Marks	Minimum Marks
1	Subject I DSC I: Python Programming Fundamentals	2	-	2	30	12	20	08
2	Subject I DSC II: Fundamentals of Cyber Security	2	-	2	30	12	20	08
3	Subject I Practical I: Practical based on Subject I DSC I	-	4	2	30	12	20	08
4	Subject II DSCI: Mathematics for Computing	2	-	2	30	12	20	08
5	Subject II DSC II: Fundamentals of Statistics	2	-	2	30	12	20	08
6	Subject II Practical I: Practical based on Subject II DSC I & Subject II DSC II	-	4	2	30	12	20	08
7	Subject III DSC I: Digital Electronics Fundamentals	2	-	2	30	12	20	08
8	Subject III DSC II: Fundamentals of Database Management Systems	2	-	2	30	12	20	08
9	Subject III Practical I: Practical based on Subject III DSC I & Subject III DSC II	-	4	2	30	12	20	08
10	OEI: Office Automation-I Lab	-	4	2	30	12	20	08
11	IKS I :Vedic Mathematics	2	-	2	30	12	20	08
	Total (A)			22	330		220	

SEMESTER-II (Duration-Six Month)								
Sr. No.	Course Code	Teaching Scheme			Examination Scheme			
		Theory and Practical			University Assessment (UA)		Internal Assessment(IA)	
		Lectures (Per week)	Hours (Per week)	Credit	Maximum Marks	Minimum Marks	Maximum Marks	Minimum Marks
1	Subject I DSC III: Computer Networks	2	-	2	30	12	20	08
2	Subject I DSC IV: Fundamentals of Cryptography	2	-	2	30	12	20	08
3	Subject I Practical II: Practical based on Subject I DSC III	-	4	2	30	12	20	08
4	Subject II DSC III: Discrete Mathematics for Cyber Security	2	-	2	30	12	20	08
5	Subject II DSC IV: Probability and Security Analytics	2	-	2	30	12	20	08
6	Subject II Practical II: Practical based on Subject II DSC III & Subject II DSC IV	-	4	2	30	12	20	08
7	Subject III DSC III: Computer Hardware and System Maintenance	2	-	2	30	12	20	08
8	Subject III DSC IV: Operating Systems Fundamentals	2	-	2	30	12	20	08
9	Subject III Practical II: Practical based on Subject III DSC III and Subject III DSC IV	-	4	2	30	12	20	08
10	OE II : Basics of HTML	-	4	2	30	12	20	08
11	VEC I: Democracy, Election and Constitution	2	-	2	30	12	20	08
	Total (B)			22	330		220	
	Total (A+B)			**44**	**660**		**440**	

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option
(NEP-2020)
PART I SEM I
Title of Course: Python Programming Fundamentals

Course Outcomes:

After completion of this course, students will be able to:

1. Understand the fundamental concepts, features, and applications of Python programming.
2. Apply variables, operators, expressions, and data types to develop Python programs.
3. Implement decision-making and iterative control structures for problem solving.
4. Utilize strings, functions, and exception handling mechanisms in Python.
5. Perform file handling operations for reading, writing, and processing data.
6. Develop simple Python programs for computational and data processing tasks.

UNIT I **(15 HOURS)**

Introduction to Python Programming

Introduction to Python, Features and Applications of Python, Installation and Execution of Python Programs, Python Interpreter and Integrated Development Environment (IDE), Structure of a Python Program, Identifiers and Keywords, Variables and Memory Concepts, Statements and Expressions, Multiple Line Statements, Comments (Single-line and Multi-line), Input and Output Operations.

Data Types and Operators

Numeric Data Types, Boolean Data Type, Strings, Type Conversion, Arithmetic Operators, Assignment Operators, Comparison Operators, Logical Operators, Bitwise Operators, Operator Precedence and Associatively.

Basic Data Structures: Lists, Tuples, Sets and Dictionaries, List Operations, Indexing and Slicing, Simple Applications of Data Structures.

UNIT II **(15 HOURS)**

Control Structures and Functions: Decision Making Statements: if, if-else, nested if, if-elif-else, Iterative Statements: while loop, for loop, Nested Loops, Loop Control Statements: break and continue, Repetition based on user input, Introduction to Functions, User-defined and Built-in Functions.

Exception Handling and File Handling

Syntax Errors and Runtime Errors, Exception Handling using try-except blocks, String Operations and Common String Functions, Introduction to Files, Types of Files, Opening and Closing Files, Reading from Files, Writing to Files, File Processing Techniques, Working with Text Files, File Handling Applications.

Reference Books

1. Learning Python, Mark Lutz, O'Reilly Publications.

2. Introduction to Computation and Programming Using Python, John V. Guttag, Prentice Hall.
3. Core Python Programming, R. Nageswara Rao, Dreamtech Press.
4. Python Programming: Using Problem Solving Approach, Reema Thareja, Oxford University Press.
5. Python Crash Course, Eric Matthes, No Starch Press.

B.Sc. Cyber Security & Digital Forensics (CS & DF)
Multiple Entry and Multiple Exit Option
(NEP-2020)
PART I SEM I
Title of course: Fundamentals of Cyber Security

Course Outcomes:

After completion of this course students will be able to;

1. Understand the basic concepts, principles, and importance of Cyber Security.
2. Explain the CIA Triad and fundamental security requirements of information systems.
3. Identify cyber threats, vulnerabilities, attacks, and security risks.
4. Understand authentication, authorization, and access control mechanisms.
5. Analyze cybercrime trends and common cyber security challenges.
6. Demonstrate awareness of cyber ethics, privacy, and safe digital practices.

UNIT I **(15 HOURS)**

Introduction to Cyber Security and Security Principles

Introduction to Cyber Security, Introduction to Digital Forensics, Role and Importance of Cyber Security and Digital Forensics, Information Security Concepts, CIA Triad (Confidentiality, Integrity and Availability), Cyber Space and Digital Assets, Threats, Vulnerabilities and Risks, Relationship between Threats, Vulnerabilities and Risks, Cyber Attack Lifecycle, Types of Cyber Attacks, Malware (Virus, Worm, Trojan Horse, Ransomware, Spyware), Phishing Attacks, Social Engineering Attacks, Password Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Defense in Depth Concept, Cyber Security Awareness and Best Practices.

UNIT II **(15 HOURS)**

Security Controls, Risk Management and Cyber Ethics

Authentication, Authorization and Accounting (AAA), Access Control Concepts, Access Control Models (DAC, MAC and RBAC), Password Security, Multi-Factor Authentication (MFA), Data Privacy and Data Protection, Basics of Risk Management, Security Policies and Procedures, Incident Reporting Concepts, Secure Web Browsing Practices, Email Security, Mobile and Social Media Security, Cyber Crimes and Cyber Criminals, Cyber Ethics, Introduction to Cyber Laws, Emerging Trends in Cyber Security and Digital Forensics.

Reference Books:

1. Cyber Security Essentials – Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short.

2. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives – Nina Godbole and Sunit Belapure.
3. Principles of Information Security – Michael E. Whitman and Herbert J. Mattord.
4. Fundamentals of Information Systems Security – David Kim and Michael G. Solomon.
5. Cybersecurity for Beginners – Raef Meeuwisse.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Practical based on Subject I DSC I

Course Outcomes

After completion of this course students will be able to:

1. Develop simple Python programs using Python IDLE.
2. Apply operators, expressions, and data types in Python programs.
3. Implement decision-making and looping constructs.
4. Utilize strings, lists, and functions in Python applications.
5. Perform file handling and exception handling operations.
6. Develop problem-solving skills using Python programming.

Lab Work

Lab work is based on Python Programming Language. This laboratory course will consist of 25 to 30 programming exercises with focus on covering the hands-on aspects covered in the theory course. Python IDLE shall be used for conducting the practical sessions.

Suggested List of Practicals

1. Installation and configuration of Python IDLE.
2. Write a program to display basic information using print statements.
3. Write a program demonstrating variables and different data types.
4. Write a program to perform arithmetic operations.
5. Write a program to calculate Simple Interest.
6. Write a program to calculate Compound Interest.
7. Write a program demonstrating type conversion.
8. Write a program using relational and logical operators.
9. Write a program to find the largest of three numbers.
10. Write a program to determine whether a number is even or odd.
11. Write a program to determine whether a year is a leap year.
12. Write a program using nested if statements.
13. Write a program to generate multiplication tables.
14. Write a program using while loop.
15. Write a program using for loop.
16. Write a program to generate Fibonacci series.
17. Write a program to calculate factorial of a number.
18. Write a program demonstrating break and continue statements.

19. Write a program to perform string operations and string slicing.
20. Write a program to count vowels and consonants in a string.
21. Write a program to check whether a string is palindrome.
22. Write a program demonstrating list operations.
23. Write a program using tuples and sets.
24. Write a program using dictionaries.
25. Write a program using user-defined functions.
26. Write a program using built-in functions.
27. Write a program to read data from a text file.
28. Write a program to write data into a text file.
29. Write a program to copy contents from one file to another.
30. Write a program demonstrating exception handling using try-except blocks.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Mathematics for Computing

Course Outcomes

After completion of this course, students will be able to:

1. Understand fundamental mathematical concepts used in computing and information technology.
2. Apply number systems and binary arithmetic in computational problems.
3. Analyze sets, functions, and logical statements used in programming and algorithm design.
4. Perform matrix operations and understand their applications in computing and artificial intelligence.
5. Apply counting techniques to solve problems related to algorithms, cyber security, and data analysis.
6. Understand the applications of graphs and trees in computer networks, cyber security, and artificial intelligence.

UNIT I **(15 HOURS)**

Number Systems and Mathematical Logic: Decimal, Binary, Octal and Hexadecimal Number Systems, Interconversion of Number Systems, Binary Arithmetic, Signed and Unsigned Numbers, Applications of Number Systems in Computing.

Sets and Functions: Sets and Set Operations, Venn Diagrams, Cartesian Product, Functions and Types of Functions, Applications of Sets and Functions in Computing.

Mathematical Logic: Statements and Propositions, Logical Connectives, Truth Tables, Tautology, Contradiction, Logical Equivalence, Applications of Logic in Programming and Algorithm Design.

UNIT II **(15 HOURS)**

Matrices and Computational Applications: Introduction to Matrices, Types of Matrices, Matrix Addition, Matrix Multiplication, Transpose of Matrix, Applications of Matrices in Computing, Data Analytics and Artificial Intelligence.

Counting Techniques: Fundamental Principle of Counting, Permutations, Combinations, Applications of Counting Techniques in Algorithms and Cyber Security.

Graphs and Trees: Introduction to Graphs, Graph Terminology, Types of Graphs, Graph Representation, Introduction to Trees, Applications of Graphs and Trees in Computer Networks, Cyber Security and Artificial Intelligence.

Reference Books

1. Discrete Mathematics and Its Applications – Kenneth H. Rosen.

2. Discrete Mathematical Structures – Tremblay and Manohar.

3. Mathematical Foundations of Computer Science – Judith L. Gersting.

4. Discrete Mathematics for Computer Scientists – Joe L. Mott, Abraham Kandel and Theodore P. Baker.

5. Higher Engineering Mathematics – B.S. Grewal.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I SEM I

Title of course: Probability Distribution

Course Outcomes:

1. Acquire knowledge of concepts of probability.
2. Understand concept of random variable and its probability distributions.
3. Apply classical, addition, multiplication, and conditional probability rules.
4. Understand and interpret probability mass functions (p.m.f.) and density functions.
5. Analyze binomial distribution and compute its mean, variance, and probabilities.
6. Evaluate Poisson distribution and apply its properties to real-life scenarios.

UNIT I **(15 HOURS)**

Probability: Trial, Sample Space, Events, Types of event, Classical definition of Probability, Addition law of probability, Conditional Probability. Multiplication law of probability, Concept of independent events. Examples without use of permutations and computations. Concept of Probability Mass Function (p.m.f) and Probability Density Function (p.d.f), Mean and variance, Simple, examples

UNIT II **(15 HOURS)**

Concept of Random variable and Probability distribution. Binomial Distribution, Definition, mean, variance, additive property of binomial distribution and examples. Poisson Distribution, Definition, mean, variance, additive property of Poisson distribution and examples. Simple examples to find probabilities and parameters. Normal Distribution Definition, mean, variance and Limiting case (binomial and Poisson distribution)Definition of Standard Normal variate and its p.d.f. Properties of normal curve, Examples to find probabilities for given area under standard normal curve.

Reference Books:-

1)Elements of Statistics by D. N. Elance.

2)Introduction to Statistics, by C.B. Gupta.

3)Mathematical Statistics, by H.C. Saxena and J.N. Kapur.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Fundamentals of Statistics

Course Outcomes

After completion of this course, students will be able to:

1. Understand basic statistical concepts and terminology.
2. Organize and present data using appropriate tabular and graphical methods.
3. Compute and interpret measures of central tendency and dispersion.
4. Analyze relationships between variables using correlation techniques.
5. Apply statistical methods to solve problems in computing, cyber security, and data analysis.
6. Interpret statistical information for informed decision-making.

UNIT I **(15 HOURS)**

Introduction to Statistics and Data Presentation: Introduction to Statistics, Types of Data, Sources of Data, Collection of Data, Classification and Tabulation of Data, Frequency Distribution, Diagrammatic and Graphical Representation of Data, Bar Diagrams, Pie Charts, Histogram, Frequency Polygon and Ogive Curves.

Measures of Central Tendency: Arithmetic Mean, Median, Mode, Weighted Mean, Applications of Measures of Central Tendency in Computing and Data Analysis.

UNIT II **(15 HOURS)**

Measures of Dispersion: Range, Quartile Deviation, Mean Deviation, Standard Deviation, Variance, Coefficient of Variation, Applications of Dispersion Measures in Data Analysis.

Correlation and Introduction to Probability: Concept of Correlation, Types of Correlation, Karl Pearson's Correlation Coefficient, Scatter Diagram, Introduction to Probability, Random Experiments, Sample Space, Events, Basic Probability Concepts and Applications.

Reference Books

1. Fundamentals of Statistics – S.C. Gupta.
2. Fundamentals of Applied Statistics – S.C. Gupta and V.K. Kapoor.
3. Business Statistics – S.P. Gupta.
4. Statistics for Management – Levin and Rubin.
5. Introduction to Probability and Statistics – Sheldon Ross.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Practical based on Subject II DSC I & Subject II DSC II

Course Outcomes

After completion of this course students will be able to:

1. Apply mathematical concepts used in computing through practical problem solving.
2. Perform number system conversions and logical operations using computational tools.
3. Utilize matrices and graph concepts for computing applications.
4. Apply statistical techniques for data organization and analysis.
5. Interpret and visualize data using spreadsheet software and programming tools.
6. Use appropriate software tools for mathematical and statistical computations.

Lab Work

Lab work is based on Mathematics for Computing and Fundamentals of Statistics. The practical course shall consist of exercises using Python IDLE, MS Excel / LibreOffice Calc, Draw.io, and other suitable computational tools.

Part A: Mathematics for Computing (10 Practicals)

Practical No.	Practical Title	Tool Used
1	Perform number system conversions (Binary, Decimal, Octal, Hexadecimal)	Python IDLE
2	Perform binary arithmetic operations	Python IDLE
3	Demonstrate set operations and Venn diagrams	Draw.io / Online Venn Diagram Tool
4	Construct truth tables for logical expressions	MS Excel
5	Verify logical connectives and logical equivalence	Python IDLE
6	Implement relations and functions for simple datasets	Python IDLE
7	Perform matrix addition and subtraction	MS Excel
8	Perform matrix multiplication	MS Excel
9	Solve permutation and combination problems	Python IDLE
10	Represent simple graphs and trees	Draw.io

Part B: Fundamentals of Statistics (10 Practicals)

Practical No.	Practical Title	Tool Used
11	Create and classify datasets	MS Excel
12	Prepare frequency distribution tables	MS Excel
13	Construct bar charts	MS Excel
14	Construct pie charts	MS Excel
15	Construct histograms	MS Excel
16	Calculate Arithmetic Mean, Median and Mode	MS Excel
17	Calculate Mean using Python programs	Python IDLE
18	Calculate Median and Mode using Python programs	Python IDLE
19	Calculate Variance and Standard Deviation	MS Excel
20	Calculate Correlation Coefficient and interpret results	MS Excel

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Digital Electronics Fundamentals

Course Outcomes

After completion of this course, students will be able to:

1. Understand the concepts of digital systems and number systems.
2. Perform conversions among binary, decimal, octal, and hexadecimal number systems.
3. Apply binary arithmetic and complement techniques in digital computations.
4. Analyze the operation of logic gates and Boolean algebra.
5. Simplify Boolean expressions using Boolean laws and Karnaugh Maps.
6. Understand the fundamentals of combinational digital circuits used in computing systems.

UNIT I **(15 HOURS)**

Number Systems and Digital Codes

Introduction to Digital Electronics, Analog and Digital Signals, Decimal, Binary, Octal and Hexadecimal Number Systems, Interconversion of Number Systems, Binary Arithmetic, Signed and Unsigned Numbers, 1's and 2's Complement, Binary Codes, Gray Code, Excess-3 Code, ASCII Code, EBCDIC Code, Parity Bit and Error Detection Concepts.

UNIT II **(15 HOURS)**

Logic Gates and Boolean Algebra

AND, OR, NOT, NAND, NOR, XOR and XNOR Gates, Symbols, Truth Tables and Applications, Boolean Algebra and Boolean Laws, De Morgan's Theorems, Universal Gates (NAND and NOR), Simplification of Boolean Expressions, Karnaugh Maps (K-Maps), Introduction to Combinational Logic Circuits, Half Adder, Full Adder, Multiplexer and Decoder.

Reference Books

1. Digital Fundamentals – Thomas L. Floyd.
2. Digital Logic and Computer Design – M. Morris Mano.
3. Fundamentals of Digital Circuits – A. Anand Kumar.
4. Digital Electronics – S. Salivahanan and S. Arivazhagan.
5. Digital Principles and Applications – Donald P. Leach.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Fundamentals of Database Management Systems

Course Outcomes

After completion of this course, students will be able to:

1. Understand the concepts and importance of database systems in modern computing environments.
2. Explain database architecture, data models, and database users.
3. Design Entity Relationship (ER) diagrams and convert them into relational schemas.
4. Apply relational database concepts, keys, and integrity constraints.
5. Write SQL statements for data definition, manipulation, and retrieval.
6. Understand database security concepts and the role of databases in Cyber Security

UNIT I **(15 HOURS)**

Introduction to Database Systems: Introduction to Database Systems, Need and Advantages of DBMS, File Processing System versus DBMS, Characteristics of Database Approach, Database Environment, Database Users and Database Administrator (DBA), Three-Schema Architecture, Database Languages (DDL, DML, DCL, TCL), Applications of Database Systems.

Data Models and Database Design: Data Models, Entity-Relationship (ER) Model, Entities, Attributes and Relationships, ER Diagrams, Mapping Cardinalities, Relational Data Model, Relational Schema, Keys (Primary Key, Candidate Key, Alternate Key, Foreign Key), Integrity Constraints, Introduction to Normalization (1NF, 2NF and 3NF).

UNIT II **(15 HOURS)**

Structured Query Language (SQL)

Introduction to SQL, Data Definition Language (DDL), Data Manipulation Language (DML), Data Control Language (DCL), Creating Databases and Tables, INSERT, UPDATE and DELETE Commands, SELECT Statement, WHERE Clause, ORDER BY Clause, DISTINCT Clause, Aggregate Functions (COUNT, SUM, AVG, MIN, MAX).

Database Security and Applications

Database Security Concepts, User Privileges and Access Control, Backup and Recovery Concepts, Introduction to Transactions, Applications of Databases in Cyber Security, Digital Forensics, Log Management, Security Monitoring Systems and Information Retrieval.

Reference Books

1. Database System Concepts – Abraham Silberschatz, Henry F. Korth and S. Sudarshan.

2. Fundamentals of Database Systems – Ramez Elmasri and Shamkant Navathe.

3. Database Management Systems – Raghu Ramakrishnan and Johannes Gehrke.

4. SQL, PL/SQL: The Programming Language of Oracle – Ivan Bayross.

5. Database Systems: Design, Implementation and Management – Carlos Coronel and Steven Morris.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER I

Title of Course: Practical based on Subject III DSC I & Subject III DSC II

Course Outcomes

After completion of this course students will be able to:

1. Apply concepts of digital electronics using hardware and simulation tools.
2. Design and analyze basic digital logic circuits.
3. Implement Boolean expressions and logic gate combinations.
4. Design and execute SQL queries on relational databases.
5. Create and manage database tables using DBMS tools.
6. Apply database concepts for information storage and retrieval.

Lab Work

Lab work is based on Digital Electronics Fundamentals and Fundamentals of Database Management Systems. The practical course shall consist of exercises using Digital Electronics Simulation Tools (CircuitVerse, Logisim, Proteus, Multisim, Tinkercad Circuits) and DBMS tools such as MySQL, SQLite, PostgreSQL or equivalent open-source database systems.

Part A: Digital Electronics Fundamentals (10 Practicals)

Practical No.	Practical Title	Tool Used
1	Verification of basic logic gates (AND, OR, NOT)	Hardware Kit / CircuitVerse
2	Verification of NAND and NOR gates	Hardware Kit / CircuitVerse
3	Verification of XOR and XNOR gates	Hardware Kit / CircuitVerse
4	Realization of basic gates using NAND gates	Hardware Kit / Logisim
5	Realization of basic gates using NOR gates	Hardware Kit / Logisim
6	Verification of De Morgan's Theorem	Hardware Kit / CircuitVerse
7	Simplification and implementation of Boolean expressions	Logisim / CircuitVerse
8	Design and implementation of Half Adder	Hardware Kit / Logisim

9	Design and implementation of Full Adder	Hardware Kit / Logisim
10	Design and implementation of Multiplexer and Decoder circuits	Hardware Kit / Logisim

Part B: Fundamentals of Database Management Systems (10 Practicals)

Practical No.	Practical Title	Tool Used
11	Installation and configuration of MySQL/SQLite	MySQL / SQLite
12	Create a database and tables using DDL commands	MySQL
13	Perform INSERT operations on tables	MySQL
14	Perform UPDATE and DELETE operations	MySQL
15	Retrieve records using SELECT statements	MySQL
16	Use WHERE, ORDER BY and DISTINCT clauses	MySQL
17	Apply aggregate functions (COUNT, SUM, AVG, MIN, MAX)	MySQL
18	Implement Primary Key and Foreign Key constraints	MySQL
19	Create simple relational database schema for a real-world application	MySQL
20	Mini database project involving table creation, data insertion and report generation	MySQL

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Computer Networks

Course Outcomes

After completion of this course, students will be able to:

1. Understand the fundamentals and applications of computer networks.
2. Identify various network topologies, transmission media, and networking devices.
3. Explain the functions of OSI and TCP/IP reference models.
4. Understand IP addressing and Internet communication mechanisms.
5. Analyze network protocols and services used in modern computer networks.
6. Apply basic network troubleshooting techniques using standard networking tools.

UNIT I **(15 HOURS)**

Introduction to Computer Networks

Introduction to Computer Networks, Need and Applications of Computer Networks, Types of Networks (PAN, LAN, MAN, WAN), Network Topologies (Bus, Star, Ring, Mesh and Tree), Transmission Media (Guided and Unguided Media), Network Devices: Hub, Switch, Bridge, Router, Gateway and Modem, Network Protocols and Standards.

OSI Reference Model

Introduction to OSI Reference Model, Functions of OSI Layers, Encapsulation and Decapsulation, Services and Protocols, Data Transmission Process in Computer Networks.

UNIT II (15 HOURS)

TCP/IP and Internet Fundamentals

TCP/IP Reference Model, Comparison of OSI and TCP/IP Models, IPv4 Addressing Concepts, Classes of IP Addresses, Subnet Mask, Network Address and Host Address, Introduction to IPv6.

Internet Services and Network Utilities, Domain Name System (DNS), Uniform Resource Locator (URL), HTTP and HTTPS Protocols, Email Protocols (SMTP, POP3 and IMAP), Introduction to Wireless Networks, Network Troubleshooting Tools: Ping, Tracert and ipconfig, Basic Concepts of Network Performance and Reliability.

Reference Books

1. Data Communications and Networking – Behrouz A. Forouzan.
2. Computer Networks – Andrew S. Tanenbaum.
3. Computer Networking: A Top-Down Approach – James F. Kurose and Keith W. Ross.\
4. Data and Computer Communications – William Stallings.
5. Introduction to Computer Networks and Cybersecurity – Chwan-Hwa Wu and J. David Irwin.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Fundamentals of Cryptography

Course Outcomes

After completion of this course, students will be able to:

1. Understand the fundamental concepts and objectives of cryptography.
2. Explain classical encryption and decryption techniques.
3. Understand modern cryptographic algorithms and key management concepts.
4. Differentiate between symmetric and asymmetric cryptographic systems.
5. Explain hashing techniques, digital signatures, and authentication mechanisms.
6. Analyze the role of cryptography in securing information and communication systems.

UNIT I **(15 HOURS)**

Introduction to Cryptography

Introduction to Cryptography, Need and Importance of Cryptography, Security Goals of Cryptography, Terminology: Plaintext, Ciphertext, Encryption, Decryption, Key, Cryptanalysis and Cryptology.

Classical Cryptographic Techniques

Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Vigenère Cipher, Rail Fence Cipher, Transposition Cipher, Advantages and Limitations of Classical Cryptography.

Symmetric Key Cryptography

Introduction to Symmetric Key Cryptography, Block Cipher and Stream Cipher Concepts, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Applications of Symmetric Key Algorithms.

UNIT II **(15 HOURS)**

Asymmetric Key Cryptography

Introduction to Public Key Cryptography, Symmetric vs Asymmetric Cryptography, RSA Algorithm (Conceptual Overview), Key Generation, Encryption and Decryption Process, Applications of Public Key Cryptography.

Hash Functions and Digital Signatures

Hashing Concepts, Characteristics of Cryptographic Hash Functions, MD5, SHA Family (Overview), Digital Signatures, Message Authentication, Digital Certificates, Public Key Infrastructure (PKI).

Applications of Cryptography

Cryptography in Network Security, Secure Communication, Email Security, E-Commerce Security, Authentication Mechanisms, Emerging Trends in Cryptography.

Reference Books

1. Cryptography and Network Security – William Stallings.
2. Network Security Essentials – William Stallings.
3. Cryptography and Information Security – V.K. Pachghare.
4. Principles of Information Security – Michael E. Whitman and Herbert J. Mattord.
5. Introduction to Modern Cryptography – Jonathan Katz and Yehuda Lindell.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Practical based on Subject I DSC III

Course Outcomes

After completion of this course students will be able to:

1. Understand networking concepts through practical implementation.
2. Configure network topologies and network devices.
3. Apply IP addressing and subnetting concepts.
4. Configure basic routing protocols in simulated environments.
5. Analyze network communication using packet analysis tools.
6. Troubleshoot basic networking problems using simulation and analysis tools.

Lab Work

Lab work is based on Computer Networks. The practical course shall consist of hands-on exercises using Cisco Packet Tracer and Wireshark.

Suggested List of Practicals

Practical No.	Practical Title	Tool Used
1	Study of networking devices and network components	Cisco Packet Tracer
2	Create and configure a simple LAN topology	Cisco Packet Tracer
3	Implement Star Network Topology	Cisco Packet Tracer
4	Implement Bus Network Topology	Cisco Packet Tracer
5	Implement Ring and Mesh Network Topologies	Cisco Packet Tracer
6	Configure IPv4 addressing for network devices	Cisco Packet Tracer
7	Perform subnetting and network address calculations	Cisco Packet Tracer
8	Configure communication between hosts using IP addressing	Cisco Packet Tracer
9	Configure routers and verify connectivity	Cisco Packet Tracer
10	Configure Static Routing between networks	Cisco Packet Tracer
11	Configure OSPF Routing Protocol and verify route propagation	Cisco Packet Tracer
12	Design and simulate a small office network	Cisco Packet Tracer
13	Configure a wireless network topology	Cisco Packet Tracer

14	Simulate client-server communication	Cisco Packet Tracer
15	Study packet flow using Simulation Mode	Cisco Packet Tracer
16	Capture packets using Wireshark	Wireshark
17	Analyze Ethernet Frames	Wireshark
18	Analyze ARP and ICMP Packets	Wireshark
19	Analyze TCP, UDP, HTTP and HTTPS Traffic	Wireshark
20	Mini Project: Design and implement a multi-network enterprise topology using IP addressing and OSPF routing	Cisco Packet Tracer

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Discrete Mathematics for Cyber Security

Course Outcomes

After completion of this course, students will be able to:

1. Apply propositional and predicate logic in cyber security problem solving.
2. Analyze mathematical structures used in computing and information security.
3. Apply counting techniques and recurrence relations in algorithm analysis.
4. Understand graph theoretic concepts used in computer networks and cyber security.
5. Apply modular arithmetic concepts used in cryptographic systems.
6. Utilize discrete mathematical concepts in cyber security and digital forensics applications.

UNIT I **(15 HOURS)**

Logic and Mathematical Structures

Propositional Logic, Predicate Logic, Logical Equivalence, Normal Forms (CNF and DNF), Rules of Inference, Proof Techniques, Mathematical Induction, Recursive Definitions and Recurrence Relations.

Relations and Algebraic Structures

Properties of Relations, Equivalence Relations, Partial Ordering Relations, Introduction to Algebraic Structures, Groups, Semigroups and Monoids, Applications in Computing and Information Security.

UNIT II **(15 HOURS)**

Modular Arithmetic and Cryptographic Foundations

Divisibility, Prime Numbers, Greatest Common Divisor (GCD), Euclidean Algorithm, Modular Arithmetic, Congruence Relations, Applications of Modular Arithmetic in Cryptography.

Graph Theory and Cyber Security Applications

Graph Terminology, Directed and Undirected Graphs, Connected Graphs, Trees and Spanning Trees, Graph Traversal Concepts, Applications of Graph Theory in Computer Networks, Cyber Security, Attack Graphs and Network Analysis.

Reference Books

1. Discrete Mathematics and Its Applications – Kenneth H. Rosen.
2. Discrete Mathematical Structures – Tremblay and Manohar.
3. Elements of Discrete Mathematics – C.L. Liu.
4. Discrete Mathematics for Computer Scientists – Joe L. Mott, Abraham Kandel and Theodore P. Baker.
5. Applied Discrete Structures – Alan Doerr and Kenneth Levasseur.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Probability and Security Analytics

Course Outcomes

After completion of this course, students will be able to:

1. Understand fundamental concepts of probability and uncertainty.
2. Apply probability distributions to real-world computing and security problems.
3. Analyze security-related data using basic statistical techniques.
4. Interpret patterns, trends, and anomalies in security data.
5. Apply analytical methods for cyber security decision-making.
6. Understand the role of data analytics in cyber security and digital forensics.

UNIT I **(15 HOURS)**

Probability Fundamentals

Random Experiments, Sample Space, Events, Types of Events, Probability Concepts, Conditional Probability, Independent Events, Bayes' Theorem, Probability Distributions, Binomial Distribution, Normal Distribution, Applications of Probability in Computing and Cyber Security.

UNIT II **(15 HOURS)**

Introduction to Security Analytics

Introduction to Security Analytics, Security Data Sources, Log Files and Event Data, Data Collection and Preprocessing, Descriptive Analytics, Data Visualization Concepts, Pattern Recognition, Anomaly Detection Concepts, Security Metrics and Indicators, Applications of Analytics in Cyber Security and Digital Forensics, Case Studies in Security Analytics.

Reference Books

1. Fundamentals of Applied Statistics – S.C. Gupta and V.K. Kapoor.
2. Introduction to Probability and Statistics – Sheldon Ross.
3. Probability and Statistics for Computer Science – James L. Johnson.
4. Data-Driven Security – Jay Jacobs and Bob Rudis.
5. Security Analytics – Mark Ryan Talabis, Robert McPherson and Inez Miyamoto.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Practical based on Subject II DSC III & Subject II DSC IV

Course Outcomes

After completion of this course students will be able to:

1. Apply discrete mathematical concepts to computing and cyber security problems.
2. Implement logical and mathematical operations using computational tools.
3. Analyze probability distributions and statistical measures.
4. Visualize and interpret security-related datasets.
5. Apply analytical techniques for identifying patterns and anomalies.
6. Use Python, Excel, and Weka for security analytics applications.

Lab Work

Lab work is based on Discrete Mathematics for Cyber Security and Probability & Security Analytics. The practical course shall consist of exercises using Python IDLE, MS Excel, Weka, Draw.io, and other suitable analytical tools.

Part A: Discrete Mathematics for Cyber Security (10 Practicals)

Practical No.	Practical Title	Tool Used
1	Construct truth tables for logical expressions	MS Excel
2	Verify logical equivalence of propositions	Python IDLE
3	Implement logical operators and Boolean expressions	Python IDLE
4	Demonstrate set operations and relations	Python IDLE
5	Implement functions and mappings for sample datasets	Python IDLE
6	Solve recursive problems using recursion	Python IDLE
7	Implement modular arithmetic operations	Python IDLE
8	Compute GCD using Euclidean Algorithm	Python IDLE
9	Represent graphs and network structures	Draw.io
10	Construct and analyze trees for hierarchical structures	Draw.io

Part B: Probability and Security Analytics (10 Practicals)

Practical No.	Practical Title	Tool Used
11	Calculate probability of simple events	Python IDLE
12	Calculate conditional probability and independent events	Python IDLE
13	Implement Bayes' Theorem for security-related scenarios	Python IDLE
14	Generate frequency distributions and statistical summaries	MS Excel
15	Calculate Mean, Median and Mode for security datasets	MS Excel
16	Calculate Variance and Standard Deviation	MS Excel
17	Visualize security event data using charts and graphs	MS Excel
18	Preprocess and explore security datasets	Weka
19	Perform classification of security-related data using machine learning tools	Weka
20	Mini Case Study: Analyze a security dataset and prepare an analytical report	Python IDLE / MS Excel / Weka

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Computer Hardware and System Maintenance

Course Outcomes

After completion of this course, students will be able to:

1. Understand the architecture and components of computer systems.
2. Identify the functions of various hardware devices and peripherals.
3. Explain memory organization and storage technologies.
4. Understand computer assembly and hardware installation procedures.
5. Perform basic troubleshooting and preventive maintenance of computer systems.
6. Apply hardware maintenance practices for efficient system operation.

UNIT I **(15 HOURS)**

Computer System Architecture

Introduction to Computer Hardware, Functional Units of a Computer System, Motherboard Components, Central Processing Unit (CPU), Arithmetic Logic Unit (ALU), Control Unit, Registers, System Bus, Input and Output Devices, Ports and Connectors, Power Supply Unit (SMPS).

Memory and Storage Devices

Primary Memory (RAM, ROM, Cache Memory), Secondary Storage Devices (Hard Disk Drive, Solid State Drive, Optical Storage Devices), Storage Hierarchy, Memory Organization, Data Storage Concepts, Backup Devices.

UNIT II **(15 HOURS)**

Computer Assembly and Peripheral Devices

Computer Assembly Concepts, Installation of Hardware Components, Expansion Cards, Printers, Scanners, Monitors, Keyboards, Mouse and Other Peripheral Devices, Device Drivers and Plug-and-Play Concepts.

System Maintenance and Troubleshooting

Preventive Maintenance, Hardware Diagnostics, Common Hardware Problems and Troubleshooting Techniques, Booting Process, BIOS and UEFI Concepts, System Configuration, Data Backup Practices, Safety Measures during Hardware Maintenance.

Reference Books

1. PC Hardware: A Beginner's Guide – Ron Gilster.
2. Upgrading and Repairing PCs – Scott Mueller.
3. Computer Hardware and Networking – B.B. Gupta.
4. Computer Fundamentals and Hardware – P.K. Sinha.
5. A+ Guide to Hardware – Jean Andrews.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Operating Systems Fundamentals

Course Outcomes

After completion of this course, students will be able to:

1. Understand the fundamental concepts and functions of operating systems.
2. Explain process management, memory management, and file management techniques.
3. Analyze scheduling methods used by operating systems.
4. Understand storage management and device management concepts.
5. Explain security and protection mechanisms in operating systems.
6. Apply operating system concepts in computing and cyber security environments.

UNIT I **(15 HOURS)**

Introduction to Operating Systems

Introduction to Operating Systems, Functions and Objectives of Operating Systems, Types of Operating Systems (Batch, Multiprogramming, Multitasking, Multiprocessing, Real-Time and Distributed Operating Systems), Operating System Structure and Services, System Calls, User Interface and Command Line Interface.

Process and Memory Management

Process Concept, Process States, Process Control Block (PCB), Process Scheduling Concepts, Scheduling Algorithms (FCFS, SJF, Round Robin), Threads and Multithreading, Memory Management Concepts, Contiguous and Non-Contiguous Memory Allocation, Virtual Memory, Paging and Segmentation.

UNIT II **(15 HOURS)**

File Systems and Device Management

File Concepts, File Organization, File Access Methods, Directory Structures, File System Management, Secondary Storage Management, Disk Scheduling Concepts, Device Management, Device Drivers, Input/Output Management.

Operating System Security and Protection

Protection and Security Concepts, Access Control, Authentication Mechanisms, User Accounts and Privileges, Malware and Operating System Threats, Backup and Recovery Concepts, Introduction to Linux and Windows Operating Systems, Role of Operating Systems in Cyber Security.

eference Books

1. Operating System Concepts – Abraham Silberschatz, Peter Baer Galvin and Greg Gagne.
2. Modern Operating Systems – Andrew S. Tanenbaum.
3. Operating Systems: Internals and Design Principles – William Stallings.
4. Fundamentals of Operating Systems – D.M. Dhamdhere.
5. Operating Systems – Harvey M. Deitel.

B.Sc. Cyber Security & Digital Forensics (CS & DF)

Multiple Entry and Multiple Exit Option (NEP-2020)

PART I – SEMESTER II

Title of Course: Practical based on Subject III DSC III & Subject III DSC IV

Course Outcomes

After completion of this course students will be able to:

1. Identify computer hardware components and their functions.
2. Understand computer system configuration and maintenance procedures.
3. Install and manage operating systems using virtual machine environments.
4. Analyze process, memory, storage, and file management concepts.
5. Configure user accounts, permissions, and security settings.
6. Apply troubleshooting and system maintenance techniques in virtual environments.

Lab Work

Lab work is based on Computer Hardware and System Maintenance and Operating Systems Fundamentals. The practical course shall consist of exercises using Virtual Machine software and suitable system administration tools.

Part A: Computer Hardware and System Maintenance (10 Practicals)

Practical No.	Practical Title
1	Study of computer hardware components and motherboard architecture
2	Identification of CPU, RAM, Storage Devices, Expansion Cards and Peripheral Devices
3	Study of BIOS/UEFI settings and system configuration
4	Creation and configuration of a Virtual Machine
5	Installation of Windows Operating System on a Virtual Machine
6	Installation of Linux Operating System on a Virtual Machine
7	Study of system boot process and startup configuration
8	Disk partitioning and storage management in a virtual environment
9	System information analysis and hardware resource monitoring
10	Troubleshooting common hardware and system startup issues

Part B: Operating Systems Fundamentals (10 Practicals)

Practical No.	Practical Title
11	Study of operating system interfaces and system utilities
12	Process management and monitoring using operating system tools
13	Memory utilization and performance monitoring
14	File and directory management operations
15	User account creation and management
16	File permissions and access control management
17	Backup and recovery operations
18	Installation and management of software packages/applications
19	Study of operating system security features and configurations
20	Mini Project: Configure and document a virtual computing environment with operating system installation, user management, storage configuration, and security settings

Suggested Tools

- Virtual Machine Software (VirtualBox / VMware / Hyper-V / Equivalent)
- Windows Operating System
- Linux Operating System (Ubuntu or Equivalent)