SYLLABUS FOR THE BATCH FROM THE YEAR 2024 TO YEAR 2025

Programme Code: DCS

Programme Name: Diploma in Cyber Security

(Semester I-II)

Examinations: 2024-2025

P.G. Department of Computer Science & Applications

Khalsa College, Amritsar

Programme name: DIPLOMA IN CYBER SECURITY
Programme code: DCS
Programme Duration 1 year

Programme Objectives

1.	To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.
2.	To help students in developing plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.
3.	To help students identify, analyze, and remediate computer security breaches.

Program Specific Outcomes (PSOs)

PSO-1.	Assess cyber-security risk management policies in order to adequately protect an organization's critical information and assets.
PSO-2.	Use several different operating systems for the development and implementation of programs in business and technical environments.
PSO-3.	Measure the performance of security systems within an enterprise-level information system. Troubleshoot, maintain and update an enterprise-level information security system.
PSO-4.	Implement cyber security solutions. Be able to use cybersecurity, information assurance, and cyber/computer forensics software/tools. Design operational and strategic cyber-security strategies and policies.

DIPLOMA IN CYBER SECURITY

Semester – I

Sr. No.	Course Code	Course Name	Distribution of The Marks				Lecture per week			Credit Distribution of The Course			Total Credit Per Course	Page No
			Theory	Practical	Internal Assessment	Total	L	T	P	L	T	P		
1	DCS-111	Fundamentals of Cyber Security	75	-	25	100	5	1	0	3	1	0	4	4-5
2	DCS-112	Cyber Security Techniques & Tools	75	-	25	100	5	1	0	3	1	0	4	6-7
3	DCS-113	Programming Using Python	75	-	25	100	5	1	0	3	1	0	4	8-9
4	DCS-114P	Lab I: - Cyber Security Techniques & Tools	-	37	13	50	0	0	6	0	0	2	2	10
5	DCS-115P	Lab II: - Programming Using Python	-	37	13	50	0	0	6	0	0	2	2	11-12
														Total Credits=16

DIPLOMA IN CYBER SECURITY

SEMESTER-I

DCS-111: Fundamentals of Cyber Security
Discipline Specific Course (DSC)

Time: 3 Hrs.

Total Marks: 100
Theory Marks: 75
Theory Internal Assessment M: 25

Credits		
L	T	P
3	1	0

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objectives:
The course is designed in a way that a candidate can

1. To protect information and information infrastructure in cyberspace.
2. Analyse security breaches
3. Remediate computer security breaches
4. Learn and implement the real-world scenarios in Cyber Investigations.

UNIT-I

Introduction to Cyber Space: History of Internet, Cyber Crime, Information Security, Computer Ethics and Security Policies, Choosing the Best Browser according to the requirement and email security,Guidelines to choose web browsers, Securing web browser, Antivirus, Email.

Cyber crime and Cyber law: Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social -engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India Case studies.

UNIT-II

Social Media Overview and Security: Introduction toSocial networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding

posting of inappropriate content, Best practices for the use of Social media

UNIT-III

Digital Devices Security,Tools and Technologies for Cyber Security: End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.

UNIT-IV

Cyber Security Threat Landscape and Techniques: Cyber Security Threat Landscape, Emerging Cyber Security threats, Cyber Security Techniques, Firewall. IT Security Act and Misc. Topics: IT Act, Hackers- Attacker Countermeasures, Web Application Security, Digital Infrastructure Security, Defensive Programming.

References:

1. Mastering Cyber Security 2022, Hack Book Works (1 January 2022);
2.Fundamentals of Network Security 1st Edition by Eric Maiwald. McGraw Hill Education (1 July 2017)
3.Cyber security by Amit Garg, Dr. Krishan Kumar Goyal. First edition (1 January 2022)

Course Outcomes:

Upon successful completion of the programme, candidates will be familiar with cyber security landscapesand able to

C0-1	Analyse and evaluate the cyber security needs of an organization.
C0-2	Protect networks and data from unauthorized access.
C0-3	Improved information security and business continuity management.
C0-4	Implement cyber security solutions and use of cyber security, information assurance,and cyber/computer forensics software/tools.
C0-5	Comprehend and execute risk management processes, risk treatment methods, and keyRisk and performance indicators
C0-6	Design and develop security architecture for an organization.
C0-7	Design operational and strategic cyber security strategies and policies

DIPLOMA IN CYBER SECURITY
SEMESTER-I
DCS-112: Cyber Security Techniques & Tools
Discipline Specific Course (DSC)

Time: 3 Hrs. **Total Marks: 100**

Theory Marks: 75

Theory Internal Assessment M: 25

Credits		
L	T	P
3	1	0

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objective:

The objective of this course is

1.	The use and application of security tools
2.	The use of security techniques
3.	Identify preferred practices for authentication, encryption, and device security
4.	The application of security techniques on real life scenarios such as cyber security consultancy and forensics.
5.	In addition to this, students will be able to improve their technical skill-sets and enhance their learning experiences through the use of various cyber tools

UNIT-I

Cyber Security Essentials: Attack Vectors, Threat, Risk and Vulnerability, Managed Detection and Response (MDR)and Cyber Kill Chain, Cyber Security Framework. Firewall and Packet Filters,. Application security, Attacks on Wireless Networks, Virtual Private Network (VPN).

UNIT-II

Application Inspection tools: Password Cracking and Brute-Force Tools Web Attack, , Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Safe Browsing Practices, IT Assets and wireless Security Cyber Security Assurance Framework, Authentication, Authorization, and Accounting, desktop Security and Malware, E-Commerce, social Engineering, Internet Crime and Act, Intellectual Property in the Cyber world.

UNIT-III

Cryptography and Encryption: Introduction, what is Cryptography? Role of Cryptography in Information Security, Components of Crypto system, Digital Signature – A Method for Information Security, Cryptographic Algorithms

Intrusion Detection for Securing the Networks: Introduction, Network Attacks – The Stages, Need for Intrusion Monitoring and Detection, Intrusion Detection for Information Systems Security

UNIT-IV

Firewalls for Network Protection: Introduction, what are Firewalls? Demilitarized Zone (DMZ), Why Firewalls are Needed – Protection Provided by Firewalls, Proxy Servers, Topologies for Different Types of Firewalls, Examining Firewalls in the Context of Intrusion Detection Systems, Firewalls vis-à-vis Routers, Design and Implementation Issues in Firewalls, Policies for Firewalls – The Importance of Using Firewalls Effectively, Compare IDS and Firewall.

References:

1. Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Author: Nina Godbole, Sunit Belapure, Publisher: Wiley.
2. India Information Systems Security – Security Management, Metrics, Frameworks and Best Practices Author: Nina Godbole, Publisher: Wiley India.
3. Cybersecurity For Beginners- Raef Meeuwisse **,** Published: May 14, 2015 by Lulu Publishing Services

Course Outcomes:

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

C0-1	Understand how important security principles must be adhered to when securing the infrastructures
C0-2	Recognize the importance of data security, maintaining data integrity,and confidentiality
C0-3	Understand the importance of balancing security, operational effectiveness and cost
C0-4	Analyze and to aptly secure the cyber perimeter of the infrastructures against cyber attacks

DIPLOMA IN CYBERSECURITY
SEMESTER-I
DCS-113: Programming-Using Python
Discipline Specific Course (DSC)

Time: 3 Hrs. **Total Marks: 100**

Credits		
L	T	P
3	1	0

Theory Marks: 75
Theory Internal Assessment M: 25

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objectives:

1	Demonstrate the ability to solve problems using system approaches, critical and innovative thinking, and technology to create solutions.
2	Understand the purpose and technology to create solutions.
3	Create scripts in Python.
4	Design and develop applications using Python.

Unit I

Python Introduction: Installing and setting Python environment, basics of Python interpreter, Execution of python program, variable, data types, and operators.
Flow control: if, if-else, for, while, range function, continue, pass, break, String Methods, Pattern Matching
Lists, Tuples and Dictionaries: Basic Operations, Iteration, Indexing, Slicing and Matrices; Dictionaries: Basic dictionary operations.

Unit-II

Functions: Definition, Call, Arguments, Scope rules and Name resolution; Recursive Function, Anonymous Function.
Standard Modules: Modules (user defined and built-in), OS and SYS, The dir () Function, Packages.
Files: Opening Files, Using Text Files.

Unit III

Exception Handling: Built-in Exception Handling Exceptions, User Defined Exceptions, Assertions in Python.

Networking: Socket module, Port Scanning, Packet Sniffing, Traffic Analysis, TCP Packet Injection. HTTP Communications with Python built in Libraries.

Unit IV

Forensic Investigations with Python: geo-locating, recovering deleted items, examining metadata and windows registry.

References:

1 . Lutz Mark, (2009). Learning Python, Latest Edition., O'REILLY Media, Inc.

2. TJ. O'Connor, Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers(2013), Elsevier.

3. Seitz Justin , (2009). Gray Hat Python: Python Programming with Hackers and Reverse Engineers, Latest Edition, No Starch Press, Inc.

4. Seitz Justin , (2015). Black Hat Python: Python Programming for Hackers and Pentesters, Latest Edition, No Starch Press, Inc

5. Berry Paul, (2011). Head First Python. Latest Edition, O'REILLY Media, Inc.

6.Introduction to Computer Science Using Python: A Computational Problem-Solving Focus, Charles Dierbach, Wiley Publications, 2012, ISBN : 978-0-470-91204-1

Course Outcomes:

CO-1	Describe the core syntax and semantics of Python programming language.
CO-2	Modules to handle multidimensional data: Numpy, Panadas
CO-3	Discover the need for working with the strings and functions.
CO-4	HTTP Communications with Python built in Libraries
CO-5	Infer the Object-oriented Programming concepts in Python.
CO-6	Examining metadata and windows registry
CO-7	To develop the ability to write database applications in Python.

DIPLOMA IN CYBER SECURITY
SEMESTER-I
DCS-114P
Lab I- Cyber Security Techniques & Tools
Skill Enhancement Course (SEC)

Credits		
L	**T**	**P**
0	**0**	**2**

Total Marks: 50
Practical Marks: 37
Practical Internal Assessment M: 13

Course Objective:

1.	The lab implementation of security tools
2.	The lab implementation of security techniques
3.	The lab implementation of applying of security techniques on real life scenarios such as cyber security consultancy and forensics with software's.
4.	In addition to this, students will be able to enhance their learning experiences through the use of various cyber tools software's.
5.	Understanding various cyber security tools.

Practical Implementation based on Cyber Security Techniques & Tools

Concepts such as strong passwords, explaining the firewall in windows and Linux

Demonstrating the various Cyber security tools such as

Comparison of Top CyberSecurity Software

1. Acunetix
2. Invicti (formerly Netsparker)
3. Wireshark
4. Norton Security
5. NMap.

Course Outcomes:

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

C0-1	Implement and understand how important security principles must be adhered to when securing the infrastructures.
C0-2	Implement in such a way that a balance of security, operational effectiveness and cost is done.
C0-3	Recognize the importance of data security, maintaining data integrity,and confidentiality
C0-4	Use Analysis tools against cyber attacks

DIPLOMA IN CYBER SECURITY
SEMESTER-I
DCS-115P
Lab II- Programming Using Python
Skill Enhancement Course (SEC)

Credits		
L	**T**	**P**
0	**0**	**2**

Total Marks: 50
Practical Marks: 37
Practical Internal Assessment M: 13

Course Objectives:

Enable the student to

1.	Understand the basics of python programming concepts.
2.	Develop programs using object-oriented features.
3.	Understand the high-performance programs designed to build up the real proficiency.
4.	To enhance logical thinking of students.

Practical Implementation based on Programming Using Python

1. Python program to print "Hello World"
2. Python program to print area of rectangle
3. Python program to print area and perimeter of circle
4. Python program to print area of right angled triangle
5. Python program to find roots of quadratic equation
6. Python program to swap two variables
7. Python program to print grade of students according to marks
8. Python Program to Check Prime Number
9. Python Program to Print all Prime Numbers in an Interval
10. Python Program to Find the Factorial of a Number
11. Python Program to Check Armstrong Number
12. Python program to print all odd numbers and even numbers of given range
13. Python program to print largest digit of a given number
14. Python program to print reverse of a given number
15. Python program to print Fibonacci series
16. Python Program to Find LCM
17. Python Program to Find HCF
18. Python Program to Make a Simple Calculator

19. Python Program to Display Calendar
20. Python program of different patterns

    For instance:

    1

    12

    123

    1234
21. Python programs related to functions
22. Python program related to lists, tuples and dictionaries

Course Outcomes:

Students will be able to

CO-1.	Describe the Control statement, String, List, and Dictionaries in Python.
CO-2.	Understand the different types of function and File handling operations.
CO-3.	Interpret Object oriented programming in Python
CO-4.	Develop and understand patterns
CO-5.	Associate python programming with real life problems

DIPLOMA IN CYBER SECURITY

SEMESTER-II

Sr. No.	Course Code	Course Name	Distribution of The Marks				Lecture per week			Credit Distribution of The Course			Total Credit Per Course	Page No
			Theory	Practical	Internal Assessment	Total	L	T	P	L	T	P		
1	DCS-121	Security & Cryptography	75	-	25	100	5	1	0	3	1	0	4	14-15
2	DCS-122	Ethical Hacking	75	-	25	100	5	1	0	3	1	0	4	16-17
3	DCS-123	Computer Hacking & Forensics	75	-	25	100	5	1	0	3	1	0	4	18-19
4	DCS-124P	Lab I - Security & Cryptography	-	37	13	50	0	0	6	0	0	2	2	20
5	DCS-125P	Lab II- Computer Hacking & Forensics	-	37	13	50	0	0	6	0	0	2	2	21
													Total Credits=16 Grand Credits(I+II)=32	

DIPLOMA IN CYBER SECURITY
SEMESTER-II
DCS-121: Security & Cryptography
Discipline Specific Course (DSC)

Time: 3 Hrs. **Total Marks: 100**

Theory Marks: 75

Theory Internal Assessment M: 25

Credits		
L	T	P
3	1	0

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objectives:

Enable the student to

1.	To understand basics of Cryptography and Network Security.
2.	To be able to secure a message over insecure channel by various means
3.	To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
4.	To understand various protocols for network security to protect against the threats in the Networks.
5.	To learn various cryptography techniques

UNIT I

Introduction to Cryptography and Block Ciphers: Introduction to security attacks, introduction to cryptography, cryptanalysis – steganography - stream and block ciphers, data encryption standard(DES) , triple DES – AES.

Confidentiality and Modular Arithmetic: Confidentiality using conventional encryption - traffic confidentiality - key distribution - random number generation.

UNIT II

Public key cryptography and Authentication requirements: Principles of public key crypto systems - RSA algorithm

Integrity checks and Authentication algorithms: MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures.

UNIT III

IP Security and Key Management) IP Security: Architecture - Authentication header - Encapsulating security payloads - combining security associations - key management.

UNIT IV

Web and System Security : Web Security: Secure socket layer and transport layer security - secure electronic transaction (SET) - System Security: Intruders - Viruses and related threads - firewall design principals – trusted systems. Open source/free/trial tools: nmap, zenmap, port scanners, network scanners

References:

1. W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education 2003.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India 2018.
3. Forouzan, TCP-IP, Protocol Suit, Tata Mc Graw Hill 2010.

Course Outcomes:

Students will be able to

CO-1.	Provide security of the data over the network.
CO-2.	Do research in the emerging areas of cryptography and network security.
CO-3.	Implement various networking protocols.
CO-4.	Protect any network from the threats in the world.
CO-5.	Understand and analyse data encryption standard, RSA and other public-key cryptosystems

DIPLOMA IN CYBER SECURITY

SEMESTER-II

DCS122: Ethical Hacking
Discipline Specific Course (DSC)

Time: 3 Hrs. **Total Marks: 100**

Credits		
L	**T**	**P**
3	**1**	**0**

Theory Marks: 75

Theory Internal Assessment M: 25

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objectives:

1.	To explore practical knowledge about ethical hacking methodology.
2.	To focus on the tools and methods for enforcement of information gathering.
3.	To understand different types of attacks and their common prevention mechanisms.
4.	To learn how to investigate attacks, technical exploits and router attacks.

UNIT I

Introduction: Understanding the importance of security, Concept of ethical hacking and essential Terminologies-Threat, Attack, Vulnerabilities. Phases involved in hacking, Hacker Types, Famous Hackers.

UNIT II

Footprinting: Introduction to footprinting, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase, Fingerprinting

UNIT III

System-Hacking: Password Hacking, Understanding Sniffers, Comprehending Active and Passive Sniffing. Metasploit- Exploits of Metasploit, Metasploit Payloads, Trojan Attacks. TCP/IP Hijacking, Email Hijacking, Email Spoofing, ARP Spoofing and Redirection, DNS and IP Sniffing. Social Engineering attacks and countermeasures,

UNIT IV

Hacking Wireless Networks: Wireless Hacking, Wireless DOS attacks, WLAN Sniffers, Hacking Tools, Securing Wireless Networks. SQL Injection and its tools, Pen Testing -Types of Penetration Testing**.**

References:

1. Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And Penetration Testing by John Slavio
2. Hacking: The Art of Exploitation by Jon Erickson
3. Mastering Hacking (The Art of Information Gathering & Scanning) by Harsh Bothra.
4. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
5. Beaver, K., Hacking for Dummies, 3rded. John Wiley & sons, 2013.

Course Outcomes:

CO-1.	To analyze and evaluate the cyber security needs.
CO-2.	To gain knowledge of the tools, techniques and ethical issues likely to face the domain of ethical hacking and ethical responsibilities.
CO-3.	To determine and analyze vulnerabilities and security solutions to reduce the risk of exploitation.
CO-4.	After the completion of the course, the students will be able to develop basic understanding of security, system attacks and defenses against them.
CO-5.	To examine how attacker to gain access of useful & sensitive information about the confidential data can do social engineering.

DIPLOMA IN CYBER SECURITY
SEMESTER-II
DCS-123: Computer Hacking & Forensics
Discipline Specific Course (DSC)

Time: 3 Hrs.

Credits		
L	**T**	**P**
3	**1**	**0**

Total Marks: 100
Theory Marks: 75
Theory Internal Assessment M: 25

Note for paper setter and students:

1. **Medium of Examination is English Language.**
2. **There will be five sections.**
3. **Section A is compulsory and will be of 15 marks consisting of 8 short answer type questions carrying 2.5 marks each covering the whole syllabus. The answer should not exceed 50 words. The students will have to attempt any 6 questions in this section.**
4. **Sections B, C, D and E will be set from units I, II, III & IV respectively and will consist of two questions of 15 marks each from the respective unit. The students are required to attempt one question from each of these sections.**

Course Objectives:

1.	To study the fundamentals of Computer Hacking
2.	To learn introduction of computer forensics,
3.	To learn to analyze and validate Forensics Data
4.	To study the tools and tactics associated with Cyber Forensics
5.	It aims at increasing the knowledge and understanding in cyber security and ethical hacking.

UNIT-I

Computer Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Windows Hacking, Linux Hacking, Types of Hacking, Trojans, Virus & Worms, Proxy & Packet Filtering , Denial of Service, Social Engineering, Physical Security, Steganography, Cryptography , Wireless Hacking , Firewall , IDS & IPS , Vulnerability, Penetration Testing, Session Hijacking, Hacking Web Servers, SQL Injection, Reverse Engineering, Email Hacking , Incident Handling & Response , Bluetooth Hacking , Mobile Phone Hacking

UNIT II

Computer Forensics Fundamentals: What is Computer Forensics?, Use of Computer Forensics in Law Enforcement, Cardinal Rules of computer forensics, Internet Artifacts, OS Artifacts and their forensic applications, Types of Computer Forensics Technology, Computer forensic analysis and validation, Network Forensic.

UNIT -III

Current Computer Forensic Tools:, Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation., Computer forensic software

tools, computer forensic hardware tools, validating and testing forensic software, Anti Forensics and probable counters,

E-mail investigations: Exploring the role of email in investigations, Email Forensic Investigation Techniques, Investigating email crimes and violations, understanding email servers, using specialized email forensic tools.

UNIT IV

Cell phone and mobile device forensics: Understanding mobile device forensic, understanding acquisition procedures for cell phones and mobile devices.

References:

1. Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And Penetration Testing ,2015, Author: John Slavio
2. Hacking. Computer Hacking, Security Testing,Penetration Testing, and Basic Security, 134 Pages · 2016 · by Gary Hall & Erin Watson
3. Baloch, R., Ethical Hacking and Penetration Testing Guide, CRC Press, 2015.
4. Beaver, K., Hacking for Dummies, 3rded. John Wiley & sons., 2013.
5. Real Digital Forensics by Keith j.Jones, Richard Bejitlich, Curtis W.Rose, AddisonWesley Pearson Education
6. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brain Jenkinson, Springer International edition.
7. Computer Evidence Collection &Presentation by Chrostopher L.T. Brown, Firewall Media.
8. Homeland Security, Techniques & Technologies by Jesus Mena, Firewall Media.
9. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M.Slade, TMH 2005
10. Windows Forensics by chad Steel, Wiley India Edition.

Course Outcomes:

After completion of this course students will be able to:

CO-1.	Learn the basic concepts of hacking and countermeasures.
CO-2.	Identify the process in taking digital evidence.
CO-3.	Describe how to conduct an investigation using methods of memory, operating system, network and email forensics.
CO-4.	Assess the different forensics tools.
CO-5.	Differentiate among different types of security attacks.
CO-6.	Describe the concept of ethical hacking.

DIPLOMA IN CYBER SECURITY
SEMESTER-II
DCS-124P Lab I - Security & Cryptography
Skill Enhancement Course (SEC)

Credits		
L	**T**	**P**
0	**0**	**2**

Total Marks: 50
Practical Marks: 37
Practical Internal Assessment M: 13

Course Objectives:

Enable the student to

1.	To understand basics of Cryptography and Network Security.
2.	To be able to secure a message over insecure channel by various means
3.	To understand the basic concepts of OSI and TCP/IP protocol
4.	To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
5.	To understand various protocols for network security to protect against the threats in the networks.

Practical Implementation based on Security & Cryptography

Course Outcomes:

Students will be able to

CO-1.	Provide security of the data over the network.
CO-2.	Understand and analyze data encryption standard, RSA and other public-key cryptosystems
CO-3.	Implement various networking protocols.
CO-4.	Protect any network from the threats in the world.

DIPLOMA IN CYBER SECURITY
SEMESTER-II
DCS125P
Lab II- Computer Hacking & Forensics
Skill Enhancement course (SEC)

Credits		
L	**T**	**P**
0	**0**	**2**

Total Marks: 50
Practical Marks: 37
Practical Internal Assessment M: 13

Course Objective:

1.	Aim of this course is to teach deep understanding of security issues and digital forensics & incident response.
2.	In addition, this course also provides the students with specialist knowledge and experience of various digital forensics techniques and incident response.
3.	It aims at increasing the knowledge and understanding in cyber security and ethical hacking through the use of certain tools.

Practical Implementation based on Hacking & Forensics.
Installation and Basic Commands of following Tools:

1. **NMAP**
2. **NESSUS**

Course Outcomes:
Upon completion of this course, the students will be able to:

CO-1.	Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response.
CO-2.	Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project.
CO-3.	Apply the knowledge to learn and use various tools.
CO-4.	Develop understanding with some hacking tools.