POST GRADUATE DIPLOMA IN CYBER SECURITY

Centre for Collaborative Programs, Training and Research,
(CCPTR, MAKAUT, WB)
Maulana Abul Kalam Azad University of Technology
(*Formerly West Bengal University of Technology*)
Main Campus: Simhat, Haringhata, Nadia-741249, WB, India
Kolkata Campus: BF-142, Sector-1,Salt Lake, Kolkata-700064

PG Diploma in CYBER SECUITY

COURSE OUTCOME

On completion of the course, students will be able to:

- PC1: The fundamental concepts of Cyber Security
- PC2: Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure.
- PC3: Design, develop, test and evaluate secure software.
- PC4: Develop policies and procedures to manage enterprise security risks.
- PC5: It helps to strengthen the contents of the program to meet the requirements of the employment market and keep the curriculum as a treasure of knowledge.

ELIGIBILITY - Graduate 10+2+3

with Mathematics & Computer Programming knowledge shall be permitted to appear and qualify for the Programme.

DURATION OF COURSE (in months) - 12 Months

COURSE CONTENT:

- Module 1 : PGDCS 101: PRINCIPLES OF CYBER SECURITY
- Module 2 : PGDCS 102: FUNDAMENTALS OF COMPUTER NETWORKING
- Module 3 : PGDCS 103: CYBER SECURITY TECHNIQUES
- Module 4 : PGDCS 201: COMPUTATIONAL NUMBER THEORY & CRYPTOGRAPHY
- Module 5 : PGDCS 202: EMERGING THREATS & DEFENCES
- Module 6 : PGDCS 203: WRITING SECURE CODE

SL.NO	MODULE TITLE	THEORY HOURS	PRACTICAL HOURS (If Applicable)	TOTAL HOURS
Module 1	PRINCIPLES OF CYBER SECURITY	28 hours	12 hours	40 hours
Module 2	FUNDAMENTALS OF COMPUTER NETWORKING	30 hours	10 hours	40 hours
Module 3	CYBER SECURITY TECHNIQUES	30 hours	10 hours	40 hours
Module 4	COMPUTATIONAL NUMBER THEORY &CRYPTOGRAPHY	30 hours	10 hours	40 hours
Module 5	EMERGING THREATS & DEFENCES	26 hours	14 hours	40 hours
Module 6	WRITING SECURE CODE	22 hours	18 hours	40 hours
TOTAL HOURS - IN HOURS - 240 Hrs. **Total theory hours** - HRS - 166 Hrs. **Total Practical Hours -** HRS - 74 Hrs				

MODULE NUMBER - PGDCS 101: PRINCIPLES OF CYBER SECURITY (40 Hours)	
THEORY (28 Hours)	
1. Introduction to Cyber Security • What's Cyber Security, CIA Triad, Potential impact of CS, CS Threats, Attacks & **Vulnerabilities**, Authorization and Access Controls, **Assessment of Vulnerabilities**, Business operations protection from threats? Job Trends.	8 Hrs
2. Network Defense Tools • Firewalls, Traffic shapers, VPN, IDS and Intrusion Detection.	6 Hrs
3. Web Application Tools • WebLOAD, Apache JMeter, ReadyAPI & Loadster. Kali Linux.	6 Hrs
4. Introduction to Cyber Crime, Law & Investigation Routers • Hacking, DOS, Phishing, Fraud, Trafficking, Stealing Identity, Password Sniffing, Cyber Crimes against Women and Children & Violating Privacy. • The World Wide Web, Web Centric Business, e-Business Architecture, Models of e-Business, e-Commerce, Threats to virtual world. **CERT-IN-** Collection, analysis and dissemination of information on cyber incidents, **IT Act 2000** - Objectives, Applicability, Non-applicability, Definitions, Amendments and Limitations.	8 Hrs
PRACTICAL (12 Hours)	
5. Implementation of Programming Languages with Basic Data Structures using JAVA/Python HTTPS	6 Hrs
6. Access Control: Implementation of Linux CLI, Hardening, Bash Scripting & Security- Kali Linux.	6 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5, 6, 2. (Comprehension) 1, 2, 3, 4, 5, 6 3. (Application) 3, 4, 5, 6 4. (Analysis) 3, 4, 5 5. (Synthesis) 2, 5, 6 6. (Evaluation) 1, 2, 3, 4, 5, 6	

MODULE NUMBER - PGDCS 102: FUNDAMENTALS OF COMPUTER NETWORKING (40 Hours)	
THEORY (30 Hours)	
1. Introduction of Computer Networking • Basic Computer Network Components – Server, client, routers, Shared Printers and other peripherals, Network Interface Card. • Types of Networks – LAN, MAN and WAN. Working of Wi-Fi and Bluetooth. Overview of cloud computing.	8 Hrs
2. Networks Standard • OSI model and TCP/IP model. Basic HTTP, World Wide Web, Web Browsers, Web Servers, Domain Names, URL and DNS.	8 Hrs
3. Transmission Media & TCP/IP. • Physical Media-different types of Cabling and Wi-Fi Architecture. TCP/UDP, IP addressing – types and classes.	6 Hrs
4. Connecting Devices, Network Topologies & Architecture. • Network Devices – hubs, Switches, routers, repeaters.	8 Hrs
PRACTICAL (10 Hours)	
5. Intrusion Detection System / Exploiting Virtual Machine	10 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5 2. (Comprehension) 1, 2, 3, 4, 5 3. (Application) 3, 4, 5 4. (Analysis) 1, 2, 3, 4, 5 5. (Synthesis) 3, 4, 5 6. (Evaluation) 3, 4, 5	

MODULE NUMBER - PGDCS 103: CYBER SECURITY TECHNIQUES (40 Hours)	
THEORY (30 Hours)	
1. Information Security & Cyber Attacks • Cybercrime against organization – Unauthorized access of computer, Password Sniffing, Denial-of-service (DOS) attack, Backdoors and Malwares and its types, E-mail Bombing, Salami Attack, Software Piracy, Industrial Espionage, Intruder attacks. • Security policies violations, Crimes related to Social Media, ATM, Online and Banking Frauds. Intellectual Property Frauds.	8 Hrs
2. Malware & Web – Application Security • Goals of Malware Analysis, Techniques Static and Dynamic Analysis, Types of Malware Backdoor, Downloader, Information Stealing malware, Scareware, Worm or Virus. SQL Injection. • Web applications interface and structure, benefits and drawbacks of web applications. Web application Vs Cloud application. Security Fundamentals: Input Validation - Attack Surface Reduction.	8 Hrs
3. Forensics & Risk Management • Digital Forensics- Introduction, Objective and Methodology, Rules of Digital Forensics. Network Forensics, Mobile Forensics, Social Media Forensics and E-mail Forensics.	6 Hrs
4. Network Security • IP security architecture, Security protocols, IPSec, Web Security – Firewalls, IDS, IDPS – Types and Technologies. Web Security: SSL Encryption, TLS, SET. Intrusion detection. Securing online payments (OTP).	8 Hrs
PRACTICAL (10 Hours)	
5. Exploit Web Application-SQL Injection.	10 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5 2. (Comprehension) 1, 2, 3, 4, 5 3. (Application) 3, 4, 5 4. (Analysis) 2, 3, 4, 5 5. (Synthesis) 3, 4, 5 6. (Evaluation) 5	

MODULE NUMBER - PGDCS 201: COMPUTATIONAL NUMBER THEORY & CRYPTOGRAPHY (40 Hours)	
THEORY (30 Hours)	
1. Computation & Complexity • P, NP and NP-completeness, Randomized computation, Space complexity, Time complexity & Average-case complexity.	8 Hrs
2. Key Management • Key management system- Key exchange, Key storage, Key use. Public and Private Keys.	6 Hrs
3. Testing Methodologies • Penetration Testing- Categories of Penetration Testing - Phases of Penetration Test - Penetration Testing Reports.	8 Hrs
4. Cryptography & Encryption • Cryptography-Definition, Model, Architecture & Process. Mechanism of Encryption & Decryption. • Data Encryption Standard (DES), Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange.	8 Hrs
PRACTICAL (10 Hours)	
5. Implementation of Programming Computation & Complexity.	5 Hrs
6. Implementation of Keys, Testing & Cryptography Methodologies.	5 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5, 6 2. (Comprehension) 1, 2, 3, 4, 5, 6 3. (Application) 5, 6 4. (Analysis) 4, 5, 6 5. (Synthesis) 3, 4, 5, 6 6. (Evaluation) 1, 2, 3, 4, 5, 6	

MODULE NUMBER - PGDCS 202: EMERGING THREATS & DEFENSES (40 Hours)	
THEORY (26 Hours)	
1. Dealing with Data Breach • Information Technology Act 2000, Digital Signature, E-Signature, Electronic Records, Electronic Evidence and Electronic Governance.	6 Hrs
2. Attacks & Defenses • Sniffing Network Traffic, Replay Attacks, Command Injection, ICMP redirect, DDoS. Defense- in-Depth Approach, Port Security, Use Encrypted Protocols, defenses with Man-in-the Middle.	8 Hrs
3. Cloud Security • Cloud Security Architecture, Identity and Access Management, Encryption and Key Management.	6 Hrs
4. Privacy Concerns • PDCA – Cycle Plan, Do, Check, Act. Types of Audit - Internal, External - Mandatory and – Statutory. ISMS 27001 ISO Standards – Introduction and Applicability.	6 Hrs
PRACTICAL (14 Hours)	
5. Implementation of Cloud Security & Privacy-Security Group, IAM, Key Management.	14 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5 2. (Comprehension) 1, 2, 3, 4, 5 3. (Application) 4, 5 4. (Analysis) 3, 4, 5 5. (Synthesis) 2, 3, 4 6. (Evaluation) 4, 5	

MODULE NUMBER - PGDCS 203: WRITING SECURE CODE (40 Hours)	
THEORY (22 Hours)	
1. Control Hijacking Attacks • Integer overflow, string vulnerabilities, Platform Defenses, Run-time Defenses.	6 Hrs
2. Isolation • Ensure Security on Code by Isolation mechanism- Encapsulation & Independencies.	6 Hrs
3. Static Analysis, Dynamic Analysis & Fuzzing • Secure Code Analysis-Static, Dynamic & Fuzzy Logic Implementation.	6 Hrs
4. Language- based Security Framework • Web-based Languages i.e. Framework of Python/R for security aspects.	4 Hrs
PRACTICAL (18 Hours)	
5. Implementation of Tools for Control Hijacking Attacks	6 Hrs
6. Implementation of Program Security & Analysis-Python/R	12 Hrs
LEARNING OUTCOME 1. (Knowledge) 1, 2, 3, 4, 5, 6 2. (Comprehension) 1, 2, 3, 4, 5, 6 3. (Application) 4, 5, 6 4. (Analysis) 2, 3, 4 5. (Synthesis) 1, 2, 3 6. (Evaluation) 5, 6	