



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Computer Engineering

Subject Code : DI05007021

Subject Name : Information Security

W.E. F. Academic Year:	2026-27
Semester:	5 th
Category of the Course:	PCC-13

Prerequisite:	Mathematics, Computer Network, Operating System, Database concepts
Rationale:	Present computing era is based on the internet; Information security is crucial for safeguarding sensitive data and protecting individuals, organizations, and nations from a wide range of threats. The rationale for information security is multifaceted and encompasses various aspects of our digital world. Protecting Confidentiality, Preserving Integrity, Ensuring Availability, Mitigating Risks, Protecting Privacy. This course aims at learning basic cryptography techniques and applying security mechanisms for operating systems as well as private and public networks to protect them from various threats.

Course Outcome: After Completion of the Course, the student will be able to:

No	Course Outcomes	RBT Level
01	Describe the fundamentals of information security.	Understanding
02	Demonstrate substitution, transposition technique and symmetric cryptography algorithm.	Apply
03	Demonstrate the public key encryption with public key cryptography.	Apply
04	Apply measures to protect the network communication from attacks using firewalls and intrusion detection systems.	Apply
05	Describe the basics of cyber security, cyber-attacks, cybercrime.	Understanding

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
L	T	PR	C	Theory		Tutorial / Practical		
				ESE (E)	PA(M)	PA(I)	ESE(V)	
3	0	2	4	70	30	20	30	150



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Computer Engineering

Subject Code : DI05007021

Subject Name : Information Security

Unit No.	Content	No. of Hours	% of Weightage
1	Introduction to Information Security Need for Security Security Goals: Confidentiality, Integrity, Availability Security Attacks: Active and Passive attacks, Denial of Service Security Services: Confidentiality, Integrity, Authentication, Non-repudiation, Access Control Security Mechanisms: Specific and Pervasive Security Mechanisms	06	15
2	Conventional and Symmetric Cryptography Introduction: Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption and Decryption. Substitution and Transposition Techniques: Monoalphabetic Cipher, Caesar Cipher, Polyalphabetic Cipher, Playfair Cipher, Hill Cipher, One Time Pad, Rail fence Steganography: Introduction, Types of steganography techniques Symmetric Cryptography: Data Encryption Standard- Structure, Advantages and Disadvantages	12	25
3	Public-Key Cryptography Principles of public-key cryptosystems, Applications of Public-key cryptosystems RSA algorithm: Description of the Algorithm, Computational aspects, Security of RSA. Public key infrastructures: Basics of digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for verifying authenticity and integrity of a certificate.	10	25
4	Network Security Security topologies: security zones, DMZ, Internet, Intranet, VLAN, Security implication, Tunneling. Firewalls: Need of Firewall, Working of Firewall, Types of Firewalls: Packet Filtering, Stateful Inspection, Application-Level Gateway, Circuit-Level Gateway and Next-Generation Firewall Intrusion detection systems (IDS): Intruders, Components of IDS, Host based IDS, Advantages and Disadvantages of HIDS, Network IDS, advantages and disadvantages of NIDS	09	20



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Computer Engineering

Subject Code : DI05007021

Subject Name : Information Security

5	Introduction to Cyber Security Introduction Cyber Threats, Cyber-attacks, Vulnerabilities, Intruders and Hackers Cyber Threats and Attacks: Worms, Virus, Ad-ware, Spyware, Trojans, Denial of Service (DoS) / Distributed DoS (DDoS), Man-in-the-Middle (MITM), IP Spoofing, ARP spoofing, SQL Injection, Phishing, Botnets, Backdoors. Cyber Crimes: Introduction to Cyber Crime, Cyberspace, Types of Cybercrime: Identity Theft, Information Theft, Hacking, Cyberstalking, Malware Distribution	08	15
	Total	45	100

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	U Level	A Level	N Level	E Level	C Level
25	50	25	0	0	0

Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)

References/Suggested Learning Resources:

(a) Books:

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson Education.
2. Weissman, J. S. (2021). Principles of Computer Security: CompTIA Security+ and Beyond Lab Manual (Exam SY0-601). McGraw-Hill Education.
3. Atul Kahate. (2019). Cryptography and Network Security (4th ed.). Tata McGraw-Hill Education.
4. Forouzan, B. A., & Mukhopadhyay, D. (2015). Cryptography and Network Security (3rd ed.). Tata McGraw-Hill Education.
5. Gollmann, D. (2011). Computer Security (3rd ed.). Wiley / Wiley India.
6. Russell, D., & Gangemi, G. T. Sr. (1991). Computer Security Basics. O'Reilly Media.

(b) Open source software and website:

1. <https://www.sans.org/information-security/>
2. <https://nptel.ac.in/>
3. <https://www.w3schools.com/cybersecurity/>
4. Software: Wireshark Traffic Analysis/Packet Sniffing Tool, Snort Packet Sniffing tool



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Computer Engineering

Subject Code : DI05007021

Subject Name : Information Security

Suggested Course Practical List:

- 1) Execute Basic TCP/IP utilities and commands. (eg: ping, ipconfig, tracert, arp, tcpdump, whois, host, netstat, nslookup, ftp, telnet)
- 2) Write a Program to implement Caesar Cipher for basic encryption and decryption. (Any of the Language C/C++/Java/Python).
- 3) Write a Program to implement Hill Cipher for basic encryption techniques. (Any of the Language C/C++/Java/Python).
- 4) Write a Program to implement the Play-Fair Cipher Technique for encryption. (Any of the Language C/C++/Java/Python).
- 5) Write a Program to implement the Rail Fence Technique for encryption. (Any of the Language C/C++/Java/Python).
- 6) Write a Program to implement RSA algorithm for asymmetric key encryption. (Any of the Language C/C++/Java/Python).
- 7) Demonstrate traffic analysis of different network protocols using tools. i.e. Wireshark.
- 8) Simulate the concept of Virtual LAN using Cisco Packet Tracer.
- 9) Simulate the concept of demilitarized zone network (DMZ) using Cisco Packet Tracer.
- 10) Simulate the working of Firewall using Cisco Packet Tracer.
- 11) Study cyber security fundamentals, including common threats and mitigation strategies.
- 12) Study of Kali Linux Operating System for cybersecurity.

List of Laboratory/Learning Resources Required:

1. Hardware: Computer with latest configuration with windows or unix os.
2. Software: C/C++/Java(Compiler), Python Interpreter, Wireshark, Cisco Packet Tracer, Kali Linux, Virtual Machines (VMware/VirtualBox) for multi-OS setup

Suggested Project List:

1. Build a password strength checker. This project helps beginners to learn about information security, as it can be done with a little bit of coding knowledge. You can use existing password strength algorithms or create your own.
2. Create a simple steganography tool that allows users to hide text or an image within another image.
3. Write a white paper on a cybersecurity topic. Writing a white paper is a great way to share your knowledge with others and establish yourself as an expert in the field.

Suggested Activities for Students:

- a) Register in Massive Open Online Courses (MOOC) on platforms such as: Swayam, edx, Coursera, Udemy etc to enhance learning.
- b) Visit to an Internet Service Provider.



GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Diploma Engineering

Level: Diploma

Branch: Computer Engineering

Subject Code : DI05007021

Subject Name : Information Security

- c) Study measures taken by IT industries.
- d) Seminars on various security tools, algorithms from the course content.
- e) Seminars on current threats of system/network.
- f) Participate in the Hackathons related to security.
