GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)
Semester -VI

Course Title: Basics of Information Security
(Course Code: 4360702)

Diploma programme in which this course is offered	Semester in which offered
Computer Engineering	6th semester

1. 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.

2. COMPETENCY

The purpose of this course is to help the student to attain the following industry identified competency through various teaching-learning experiences:

- **Evaluate and apply diverse cryptographic techniques to safeguard networked systems, integrating foundational knowledge of basic information systems and principles of cyber security.**

3. COURSE OUTCOMES (COs)

The theory should be taught and practical should be carried out in such a manner that students are able to acquire different learning outcomes in cognitive, psychomotor and affective domain to demonstrate following course outcomes:

a) Describe fundamentals of information security.
b) Demonstrate substitution, transposition technique and symmetric cryptography algorithm.
c) Demonstrate the public key encryption with public key cryptography.
d) Apply measures to protect the network communication from attacks using firewalls and intrusion detection systems.
e) Describe the basics of cyber security, cyber attacks, cyber crime.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme (In Hours)			Total Credits (L+T/2+P/2)	Examination Scheme				
				Theory Marks		Practical Marks		Total Marks
L	T	P	C	CA	ESE	CA	ESE	
3	-	2	4	30	70	25	25	150

(*): Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

***Legends: L**-Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** -Practical; **C** – Credit, **CA** - Continuous Assessment; **ESE** -End Semester Examination.*

5. SUGGESTED PRACTICAL EXERCISES

The following practical outcomes (PrOs) are the subcomponents of the COs. These PrOs need to be attained to achieve the COs.

Sr. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. required
1	Execute Basic TCP/IP utilities and commands. (eg: ping, ipconfig, tracert, arp, tcpdump, whois, host, netstat, nslookup, ftp, telnet etc...)	I	02
2	Write a Program to implement Caesar Cipher for basic encryption and decryption. (Any of the Language C/C++/Java/Python)	II	02
3	Write a Program to implement Hill Cipher for basic encryption techniques. (Any of the Language C/C++/Java/Python)	II	04
4	Write a Program to implement the Play-Fair Cipher Technique for encryption. (Any of the Language C/C++/Java/Python)	II	02
5	Write a Program to implement the Rail Fence Technique for encryption. (Any of the Language C/C++/Java/Python)	II	02
6	Write a Program to implement RSA algorithm for asymmetric key encryption. (Any of the Language C/C++/Java/Python)	III	02
7	Demonstrate traffic analysis of different network protocols using tools. i.e. Wireshark.	IV	04
8	Simulate the concept of Virtual LAN using Cisco Packet Tracer.	IV	02
9	Simulate the concept of demilitarized zone network (DMZ) using Cisco Packet Tracer.	IV	02
10	Simulate the working of Firewall using Cisco Packet Tracer.	IV	02
11	Study cyber security fundamentals, including common threats and mitigation strategies.	V	02

12	Study of Kali Linux Operating System for cybersecurity.	V	02
	Total		28

Note

*i. More **Practical Exercises** can be designed and offered by the respective course teacher to develop the industry relevant skills/outcomes to match the COs. The above table is only a suggestive list.*

*ii. The following are some **sample** 'Process' and 'Product' related skills (more may be added/deleted depending on the course) that occur in the above listed **Practical Exercises** of this course required which are embedded in the COs and ultimately the competency.*

S. No.	Sample Performance Indicators for the PrOs	Weightage in %
1	Regularity	20
2	Problem Analysis	20
3	Development of the Solution	20
4	Testing of the Solution	20
5	Mock viva test	20
Total		**100**

6. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

1. Hardware: Computer System with latest configuration and laptops
2. Software: C/C++/Java(Compiler), Python Interpreter, Wireshark, Cisco Packet Tracer, Kali Linux

7. AFFECTIVE DOMAIN OUTCOMES

The following ***sample*** Affective Domain Outcomes (ADOs) are embedded in many of the above-mentioned COs and PrOs. More could be added to fulfill the development of this competency.

a) Work as an Information Security Analyst.
b) Follow ethical practices.
c) Complying with procedures.
d) Work collaboratively in a team.
e) Workforce capable of preventing and mitigating cyber-attacks.

The ADOs are best developed through the laboratory/field based exercises. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

i. 'Valuing Level' in 1st year
ii. 'Organization Level' in 2nd year.
iii. 'Characterization Level' in 3rd year.

8. UNDERPINNING THEORY

Only the major Underpinning Theory is formulated as higher-level UOs of *Revised Bloom's taxonomy* in order development of the COs and competency is not missed out by the students and teachers. If required, more such higher-level UOs could be included by the course teacher to focus on the attainment of COs and competency.

Unit	Unit Outcomes (UOs) (4 to 6 UOs at Application and above level)	Topics and Sub-topics
Unit – I Introduction to Information Security	1.a Describe basic concept of Information Security and security attacks	1.1 Introduction to Information Security 1.2 Need for Security 1.3 Security Attacks : Active, Passive and Denial of Service 1.4 Security Basics : Confidentiality, Integrity and Availability 1.5 Services and Mechanisms
Unit – II Conventional and Symmetric Cryptography	2.a Encrypt and Decrypt the given text using different substitution methods. 2.b Describe the given technique of cryptography using an example.	2.1 Introduction: Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption and Decryption. 2.2 Substitution and Transposition Techniques: Monoalphabetic Cipher, Caesar Cipher, Polyalphabetic Cipher, Playfair Cipher, Hill Cipher, One Time Pad, Rail fence 2.3 Steganography: Introduction, Types of steganography techniques 2.4 Symmetric Cryptography : Data Encryption Standard- Structure, Advantages and Disadvantages
Unit– III Public key Cryptography	3.a Describe Public-Key Cryptography and its applications. 3.b Describe the RSA algorithm with its working. 3.c Describe digital signature and working of Public Key Infrastructure	3.1 Public-Key Cryptography : Principles of public-key cryptosystems, Applications of Public-key cryptosystems 3.2 The RSA algorithm: Description of the Algorithm, Computational aspects, Security of RSA. 3.3 Public key infrastructures : basics digital signatures, digital certificates, certificate authorities, registration authorities, steps for obtaining a digital certificate, steps for

		verifying authenticity and integrity of a certificate
Unit– IV Network Security	4.a Describe the security topologies. 4.b Explain function of Firewall and different types of Firewall. 4.c Distinguish various types of IDS with advantages and disadvantages.	4.1 Security topologies – security zones, DMZ, Internet, Intranet, VLAN, Security implication, Tunneling. 4.2 Firewalls: Need of Firewall, Working of Firewall, Types of Firewall: Packet Filtering, Stateful Inspection, Application Level Gateway, Circuit-Level Gateway and Next-Generation Firewall 4.3 Intrusion detection systems (IDS): Intruders, Components of IDS, Host based IDS: Host based IDS, Advantages and Disadvantages of HIDS, Network based IDS: Network IDS, advantages and disadvantages of NIDS
Unit– V Cyber Security	5.a Describe basic concepts of cyber security and Network threats. 5.b Describe Cyber crime and problems associated with computer crime	5.1 Introduction to Cyber Security, Cyber Threats, Types of Cyber Attacks, Vulnerabilities, Intruders and Hackers, Threats: Worms, Virus, Ad- ware, Spy-ware, Trojans and covert channels, Backdoors, Bots, IP Spoofing, ARP spoofing, Session Hijacking 5.2 Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Traditional Problems Associated with Computer Crime

***Note**: The UOs need to be formulated at the 'Application Level' and above of Revised Bloom's Taxonomy' to accelerate the attainment of the COs and the competency.*

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	**Introduction to Information Security**	06	4	2	2	8
II	**Conventional and Symmetric Cryptography**	12	2	6	12	20
III	**Public key Cryptography**	10	2	8	6	16

IV	**Network Security**	10	4	6	6	16
V	**Cyber Security**	04	4	4	2	10
Total		**42**	**16**	**26**	**28**	**70**

Legends: *R=Remember, U=Understand, A=Apply and above (Revised Bloom's taxonomy)*
Note*: This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.*

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related ***co-curricular*** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

a) Visit to an Internet Service Provider.
b) Study measures are taken by small computer industries.
c) Seminars on various security tools, algorithms from the course content.
d) Seminars on current threats of system/network.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various outcomes in this course:

a) Massive open online courses (***MOOCs***) may be used to teach various topics/subtopics.
b) Guide student(s) in undertaking micro-projects.
c) ***'L' in section No. 4*** means different types of teaching methods that are to be employed by teachers to develop the outcomes.
d) About ***20% of the topics/sub-topics*** which are relatively simpler or descriptive in nature is to be given to the students for ***self-learning***, but to be assessed using different assessment methods.
e) With respect to ***section No.10***, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project are group-based. However, in the fifth and sixth semesters, it should be preferably be ***individually*** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In special situations where groups have to be formed for micro-projects, the number of students in the group should ***not exceed three.***

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain a dated work diary consisting of individual contributions in the

project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than ***16 (sixteen) student engagement hours*** during the course. The student ought to submit a micro-project by the end of the semester to develop the industry oriented COs.

A suggestive list of micro-projects is given here. This has to match the competency and the COs. Similar micro-projects could be added by the concerned course teacher:

- **Project idea 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.
- **Project idea 2:** Create a simple steganography tool that allows users to hide text or an image within another image.
- **Project idea 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.

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Author	Publication with place, year and ISBN
1	Cryptography and Network Security Principles and Practices	Williams Stallings	Pearson Education, Third Edition
2	Principles of Computer Security CompTIA Security+ and Beyond Lab Manual	Vincent Nestler, Gregory White, Wm. Arthur Conklin, Matthew Hirsch, Corey Schou	Tata-McGraw Hill
3	Cryptography and Network Security Principal and Practices	Atul Kahate	Tata-McGraw-Hill
4	Cryptography and Network Security	B A Forouzan	Tata-McGraw-Hill
5	Computer Security Basics	Deborah Russell G.T. Gangenisr	O'Reilly publication
6	Computer Security	Dieter Gollman	Wiley India Education,

14. SOFTWARE/LEARNING WEBSITES

a. https://www.sans.org/information-security/
b. https://nptel.ac.in/
c. https://www.coursera.org/
d. https://www.w3schools.com/cybersecurity/
e. Software: Wireshark Traffic Analysis/Packet Sniffing Tool, Snort Packet Sniffing tool

15. PO-COMPETENCY-CO MAPPING

Semester VI	Basics of Information Security(Course Code: 4360702)
	POs and PSOs

Competency & Course Outcomes	PO 1 Basic & Discipline specific knowledge	PO 2 Problem Analysis	PO 3 Design/ development of solutions	PO 4 Engineering Tools, Experimentation & Testing	PO 5 Engineering practices for society, sustainability & environment	PO 6 Project Management	PO 7 Life-long learning
Competency ● Evaluate and apply diverse cryptographic techniques to safeguard networked systems, integrating foundational knowledge of basic information systems and principles of cyber security.							
Course Outcomes **CO a)** Describe fundamentals of information security.	3	-	-	-	3	-	3
CO b) Demonstrate substitution, transposition technique and symmetric cryptography algorithm.	3	2	3	2	-	2	3
CO c) Demonstrate the public key encryption with public key cryptography.	3	3	3	3	-	3	3
CO d) Apply measures to protect the network communication from attacks using firewalls and intrusion detection systems.	3	3	3	3	-	3	3
CO e) Describe the basics of cyber security, cyber attacks, cyber crime.	3	2	2	3	3	-	3

Legend: '**3'** for high, '**2**' for medium, **'1'** for low or **'-'** for the relevant correlation of each competency, CO, with PO/ PSO

16. COURSE CURRICULUM DEVELOPMENT COMMITTEE

GTU Resource Persons

Sr. No.	Name and Designation	Institute	Email
1	Ms. Manisha P. Mehta (HOD)	Government Polytechnic Himmatnagar	manishamehtain@gmail.com
2	Mrs. M. V. Prajapati - Lect.(CE)	Government Polytechnic Gandhinagar	mvprajapati2014@gmail.com
3	Mr. Amit S. Vaishnav - Lect.(CE)	Government Polytechnic Gandhinagar	amitvaishnav1112@gmail.com
4	Mr. Punit Saswadkar - Lect.(CE)	Government Polytechnic Gandhinagar	psgpg20@gmail.com