Program Name : **Computer Engineering Program Group/ Diploma in Artificial Intelligence and Machine Learning / Diploma in Computer Hardware & Maintenance / Diploma in Electronics and Computer Engineering / Diploma in Cloud Computing and Big Data**

Program Code : **CO/CM/IF/CW/AN/BD/HA/TE**

Semester : **Sixth**

Course Title : **Network and Information Security**

Course Code : **22620**

1. RATIONALE

Computer network security is an important aspect in today's world. Now days due to various threats designing security in organization is an important consideration. It is essential to understand basic security principles, various threats to security and techniques to address these threats. The student will be able to recognize potential threats to confidentiality, integrity and availability and also able to implement various computer security policies. This course will introduce basic cryptographic techniques, fundamentals of computer/network security, Risks faced by computers and networks, security mechanisms, operating system security, secure System design principles, and network security principles. Also it will create awareness about IT ACT and different Cyber laws.

2. COMPETENCY

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

- **Maintain Network and Information security of an organization.**

3. COURSE OUTCOMES (COs)

The theory, practical experiences and relevant soft skills associated with this course are to be taught and implemented, so that the student demonstrates the following ***industry oriented*** COs associated with the above mentioned competency:

a) Identify risks related to Computer security and Information hazard in various situations.
b) Apply user identification and authentication methods.
c) Apply cryptographic algorithms and protocols to maintain Computer Security.
d) Apply measures to prevent attacks on network using firewall.
e) Maintain secured networks and describe Information Security Compliance standards.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit (L+T+P)	Examination Scheme											
				Theory						Practical					
L	T	P		Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	20

(*): Under the theory PA, Out of 30 marks, 10 marks are for micro-project assessment to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessment of the UOs required for the attainment of the COs.
Legends: ***L****-Lecture;* ***T*** *– Tutorial/Teacher Guided Theory Practice;* ***P*** *-Practical;* ***C*** *– Credit,****ESE*** *-End Semester Examination;* ***PA*** *- Progressive Assessment*

5. COURSE MAP (with sample COs, PrOs, UOs, ADOs and topics)

This course map illustrates an overview of the flow and linkages of the topics at various levels of outcomes (details in subsequent sections) to be attained by the student by the end of the course, in all domains of learning in terms of the industry/employer identified competency depicted at the centre of this map.

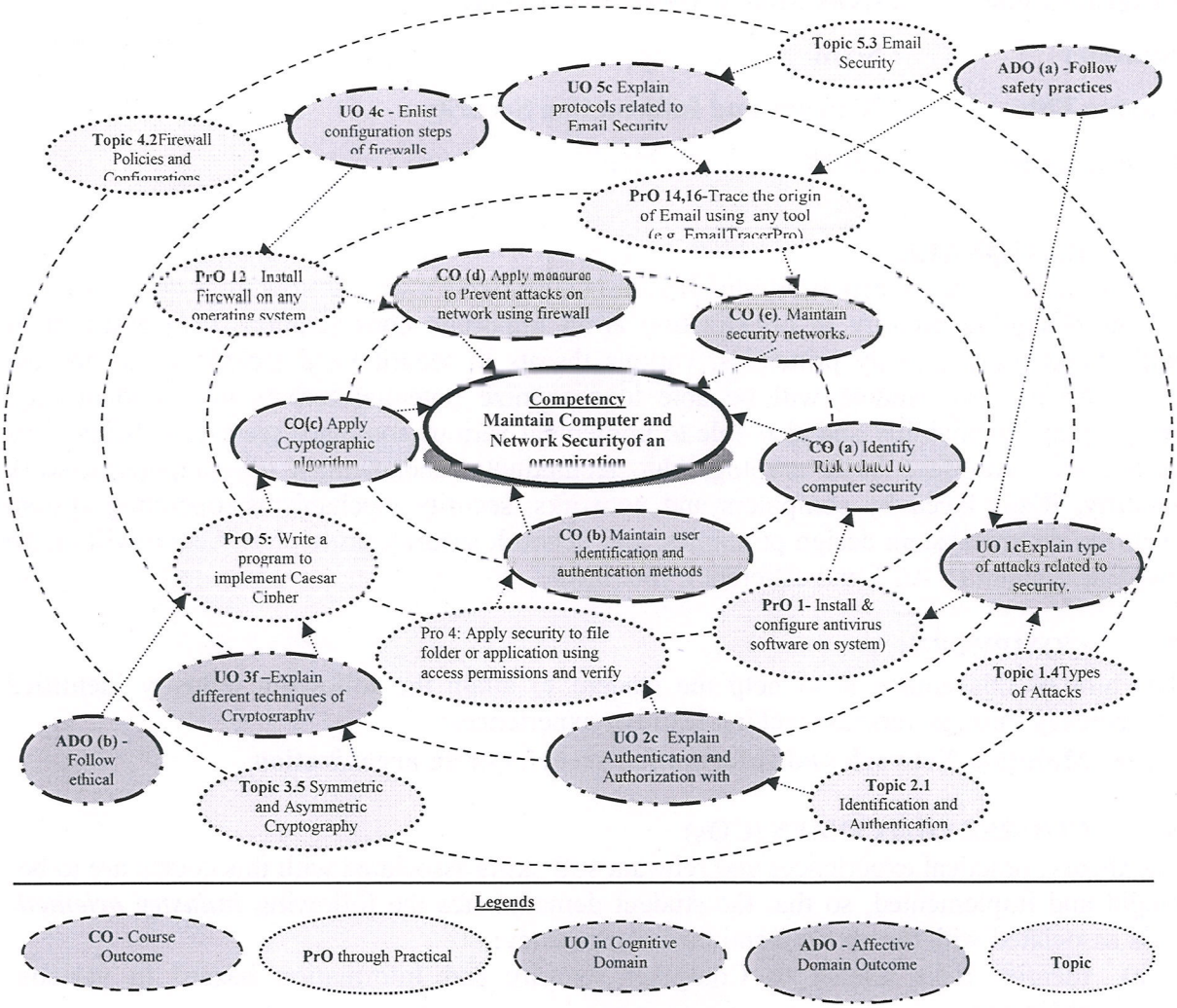

Figure 1 - Course Map

6. SUGGESTED PRACTICALS/ EXERCISES

The practicals in this section are PrOs (i.e. sub-components of the COs) to be developed and assessed in the student for the attainment of the competency.

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
1	a. Install and configure Antivirus software on system (any). b. Set up operating system Updates.	I	2
2	Perform Backup and Restore of the system.	I	2
3	Set up passwords to operating system and applications.	II	2
4	Apply security to file folder or application using access permissions and verify.	II	2
5	Write a program to implement Caesar Cipher	III	2
6	Write a program to implement Vernam Cipher	III	2

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
7	Create and verify Hash Code for given message	III	2
8	Write a program to implement Rail fence technique	III	2
9	Write a program to implement Simple Columnar Transposition technique	III	2
10	Create and verify digital signature using tool (e.g. Cryptool)	III	2
11	Use Steganography to encode and decode the message using any tool.	III	2
12	a. Install firewall on any operating system. b. Configure firewall settings on any operating system.	IV	2
13	Create and verify Digital Certificate using tool (e.g. Cryptool)	V	2
14	Trace the origin of Email using any tool(e.g. emailTrackerPro)	V	2
15	Trace the path of web site using Tracert Utility	V	2
16	PGP Email Security a. Generate Public and Private Key Pair. b. Encrypt and Decrypt message using key pair.	V	2
		Total	**32**

Note

i. A suggestive list of PrOs is given in the above table. More such PrOs can be added to attain the COs and competency. All the above listed practical need to be performed compulsorily, so that the student reaches the 'Applying Level' of Blooms's 'Cognitive Domain Taxonomy' as generally required by the industry.

ii. The 'Process' and 'Product' related skills associated with each PrO are to be assessed according to a suggested sample given below:

S. No.	Performance Indicators	Weightage in %
1	Correctness of the flow of procedures.	40
2	Debugging ability.	20
3	Quality of input and output displayed (messaging and formatting)	10
4	Answer to sample questions	20
5	Submission of report in time	10
Total		**100**

The above PrOs also comprise of the following social skills/attitudes which are Affective Domain Outcomes (ADOs) that are best developed through the laboratory/field based experiences:

a) Work collaboratively in team
b) Follow ethical Practices.

The ADOs are not specific to any one PrO, but are embedded in many PrOs. Hence, the acquisition of the ADOs takes place gradually in the student when s/he undertakes a series of practical experiences over a period of time. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

- 'Valuing Level' in 1st year
- 'Organization Level' in 2nd year.
- 'Characterization Level' in 3rd year.

7. MAJOR EQUIPMENT/ INSTRUMENTSREQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of practicals, as well as aid to procure equipment by authorities concerned.

S. No.	Equipment Name with Broad Specifications	PrO. S. No.
1	Computer system (Any computer system with basic configuration)	All
2	Antivirus Software(any)	
3	Any compiler	6,7,8,9
4	Encryption Decryption tool(preferably Open source based)	10,13
5	Steganography Tools. (preferably Open source based)	11
6	E-mail tracing Tools. (preferably Open source based)	14
7	Web tracing Tools. (preferably Open source based)	15

8. UNDERPINNING THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to develop UOs in cognitive domain for achieving the COs to attain the identified competency. More UOs could be added.

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit – I Introduction to Computer and Information Security	1a. Explain the importance of the given component of computer security. 1b. Explain the characteristics of the given type of threat. 1c. Explain the given type of attacks related with security. 1d. Describe the features of given type of update of operating system. 1e. Classify Information. 1f. Explain Principles of Information Security.	1.1 Foundations of Computer Security: Definition and Need of computer security, Security Basics: Confidentiality, Integrity, Availability, Accountability, Non-Repudiation and Reliability. 1.2 Risk and Threat Analysis: Assets, Vulnerability, Threats, Risks, Counter measures. 1.3 Threat to Security: Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan Horse, Intruders, Insiders. 1.4 Type of Attacks: Active and Passive attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Encryption attacks. 1.5 Operating system security: Operating system updates : HotFix, Patch, Service Pack. 1.6 Information, Need and Importance of Information, information classification, criteria for information classification, Security, need of security, Basics principles of information security.

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit– II User Authentication and Access Control	2a. Explain techniques of the given type of attack on passwords. 2b. Explain mechanism of the given type of Biometric. 2c. Apply the relevant Authentication method for the given situation with an example. 2d. Describe features of the given access control policy.	2.1 Identification and Authentication: User name and Password, Guessing password, Password attacks-Piggybacking, Shoulder surfing, Dumpster diving. 2.2 Biometrics: Finger Prints, Hand prints, Retina, patterns, Voice patterns, Signature and Writing patterns, Keystrokes. 2.3 Access controls: Definition, Authentication Mechanism, principle-Authentication, Authorization, Audit, Policies: DAC, MAC,RBAC.
Unit– III Cryptography	3a. Encrypt/Decrypt the given text using different substitution techniques. 3b. Convert plain text to cipher text and vice versa using the given transposition technique. 3c. Convert the given message using steganography. 3d. Explain the given technique of cryptography using example.	3.1 Introduction: Plain Text, Cipher Text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption. 3.2 Substitution Techniques: Caesar's cipher, Modified Caesar's Cipher, Transposition Techniques: Simple Columnar Transposition. 3.3 Steganography : Procedure 3.4 Symmetric and Asymmetric cryptography: Introduction to Symmetric encryption, DES (Data encryption Standard) algorithm, Asymmetric key cryptography: Digital Signature.
Unit-IV Firewall and Intrusion Detection System	4a. Compare types of firewall on the given parameter(s). 4b. Explain function of the given type of firewall configuration. 4c. Compare various IDS techniques on the given parameter(s). 4d. Describe features of the given IDS technique.	4.1 Firewall : Need of Firewall, types of firewall- Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. 4.2 Firewall Policies, Configuration, limitations, DMZ. 4.3 Intrusion Detection System : Vulnerability Assessment, Misuse detection, Anomaly Detection, Network-Based IDS, Host-Based IDS, Honeypots
Unit –V Network Security, Cyber Laws and Compliance Standards.	5a. Explain the given component of Kerberos authentication protocol. 5b. Explain the given IP Security protocol with modes. 5c. Explain working of the given protocol for Email security. 5d. Describe the given component of Public Key Infrastructure. 5e. Classify the given Cyber crime.	5.1 Kerberos : Working, AS, TGS, SS 5.2 IP Security- Overview, Protocols- AH, ESP, Modes- transport and Tunnel. 5.3 Email security- SMTP, PEM, PGP. 5.4 Public key infrastructure (PKI): Introduction, Certificates, Certificate authority, Registration Authority, X.509/PKIX certificate format. 5.5 Cyber Crime: Introduction, Hacking , Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography , Identity Theft and Fraud , Cyber terrorism, Cyber Defamation. 5.6 Cyber Laws: Introduction, need,

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
	5f. Explain the specified Cyber law. 5g. Describe compliance standards for Information Security.	Categories: Crime against Individual, Government, Property. 5.7 Compliance standards: Implementing and Information Security Management System, ISO 27001, ISO 20000, BS 25999, PCI DSS, ITIL framework, COBIT framework.

***Note**:To attain the COs and competency, above listed UOs need to be undertaken to achieve the 'Application Level' of Bloom's 'Cognitive Domain Taxonomy'*

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 Computer and Information Security	12	06	06	02	14
II	User Authentication and Access Control	06	04	04	02	10
III	Cryptography	06	02	04	08	14
IV	Firewall and Intrusion Detection System	12	04	06	08	18
V	Network Security, Cyber Laws and Compliance Standards.	12	06	06	02	14
	Total	**48**	**22**	**26**	**22**	**70**

Legends: R=Remember, U=Understand, *A=Apply and above (Bloom's Revised taxonomy)*
***Note**: This specification table provides general guidelines to assist student for their learning and to teachers to teach and assess students with respect to attainment of UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from 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) Prepare journal of practicals.
b) Undertake micro-projects.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

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

a) Massive open online courses (***MOOCs***) may be used to teach various topics/sub topics.
b) ***'L' in item No. 4*** does not mean only the traditional lecture method, but different types of teaching methods and media that are to be employed to develop the outcomes.
c) About ***15-20% of the topics/sub-topics*** which is relatively simpler or descriptive in nature is to be given to the students for ***self-directed learning*** and assess the

development of the COs through classroom presentations (see implementation guideline for details).

d) With respect to item No.10, teachers need to ensure to create opportunities and provisions for ***co-curricular activities***.
e) Guide student(s) in undertaking micro-projects.
f) Demonstrate students thoroughly before they start doing the practice.
g) Encourage students to refer different websites to have deeper understanding of the subject.
h) Observe continuously and monitor the performance of students in Lab.

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 is 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 dated work diary consisting of individual contribution 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 micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. Similar micro-projects could be added by the concerned faculty:

a) Case Studies in Secure Computing: Achievements and Trends.
b) Implement Client/Server communication using cryptography tools in your laboratory.
c) Create digital certificate for your departmental/ personal communication.
d) Implement communication system using steganography. Encrypt image and message using any cryptography technique.
e) Implement communication system using steganography using audio files. Encrypt audiofile and message using any cryptography technique.
f) Implement Three Level Password Authentication System.
g) Any other micro-projects suggested by subject faculty on similar line.

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Author	Publication
1	Computer Security	Dieter Gollmann	Wiley Publication, New Delhi, ISBN : 978-0-470-74115-3
2	Cryptography and Network Security	Atul Kahate	McGraw Hill Education, New Delhi ISBN: 978-1-25-902988-2
3	Cyber Laws And IT Protection	Harish Chander	PHI Publication,New Delhi, 2012 ISBN: 978-81-203-4570-6
4	Implementing Information Security based on ISO 27001 / ISO 27002 (Best Practice)	Alan Calder	Van Haren Publishing ISBN-13: 978-9087535414 ISBN-10: 9087535414

14. SOFTWARE/LEARNING WEBSITES

a) http://nptel.ac.in/courses/106105162/
b) https://www.tutorialspoint.com//computer_security/computer_security_quick_guide.htm
c) http://learnthat.com/introduction-to-network-security/
d) https://freevideolectures.com/course/3027/cryptography-and-network-security
e) https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/
f) http://stylesuxx.github.io/steganography/
g) https://smartninja-pgp.appspot.com/
h) http://www.cyberlawsindia.net/cyber-india.html
i) https://www.upcounsel.com/cyber-law
j) http://cyberlaws.net/cyber-law/