GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Minor/Hons. Program

Level: UG

Branch: Minor/Hons. Cyber Security

Course / Subject Code : BE040AH011

Course / Subject Name : Information Theory for Cyber Security

w. e. f. Academic Year:	2025-26
Semester:	4th
Category of the Course:	Core Courses

Prerequisite:	Computer Networks, Engineering Mathematics
Rationale:	The information exchanged through the Internet plays a vital role for their owners and the security of such information/data is of prime importance. Knowing the concepts, principles and mechanisms for providing security to the information/data is very important for the students. This course focuses on secure communication built on information theory. The subject covers various important topics concerning information security like information theory, symmetric and asymmetric cryptography and secret key agreement. Various information metrics for security will be compared.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	% of Weightage
01	To introduce the principles and applications of information theory.	20
02	To introduce cryptography, key distribution and public key infrastructure.	50
03	To learn coding schemes, including error correcting codes.	15
04	Student able to understand cyber-attack, vulnerabilities and ways to find it by scanning any system/network.	15

Teaching and Examination Scheme:

Teaching - Learning Scheme (in Hours per Semester)					Total Credits = TH/30	Assessment Pattern and Marks					Total Marks
						Theory		Tutorial / Practical			
L	T	P	PWL	TH		ESE (E)	PA (M)	PA/ (I)	PBL(I)	ESE (V)	
45	0	30	45	120	04	70	00	00	30	50	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1.	Shannon's foundation of Information theory, Lower bounds on key size: secrecy, authentication and secret sharing. provable security, computationally secure, symmetric cipher.	5	10
2.	Secrecy, Authentication, Secret sharing, Optimistic results on perfect secrecy, Secret key agreement, Unconditional Security, Quantum Cryptography.	5	10
3.	Information-theoretic security and cryptography, basic introduction to Diffie-Hellman, AES, and side-channel attacks.	8	19
4.	Secrecy metrics: strong, weak, semantic security, partial secrecy, Secure source coding: rate-distortion theory for secrecy systems, side information at receivers, Differential privacy, Distributed channel synthesis.	8	18
5.	Digital and network forensics, Public Key Infrastructure, Lightweight cryptography, Elliptic Curve Cryptography and applications.	8	18
6.	Vulnerability scanning for cyber security, Open Port/ Service Identification, Banner / Version Check. Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – Nmap, THC-Amap and System tools. Network Sniffers and Injection tools – Tcpdump and Windump, Wireshark.	11	25
	Total	**45**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
35	35	15	10	5	

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

References/Suggested Learning Resources:

Books:

1. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons.
2. Communication Systems: Analog and digital, Singh and Sapre, Tata McGraw Hill.
3. Fundamentals in information theory and coding, Monica Borda, Springer
4. Information Theory, Coding and Cryptography R Bose.
5. Multi-media System Design, Prabhat K Andleigh and Kiran Thakrar.
6. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
7. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sunit Belpure, Publication Wiley

Suggested Course Practical List: If any

1. TCP scanning and Port scanning using NMAP.
2. Implement packet tracing using Wireshark.
3. Implement Playfair cipher encryption-decryption.
4. Implement Polyalphabetic cipher encryption-decryption.
5. Write a program that demonstrates the use of Hamming Code.
6. Write a program that illustrates the working elliptic curve cryptography.
7. Implement Diffie-Hellman Key exchange Method.
8. Implement RSA encryption-decryption algorithm.
9. Perform various encryption-decryption techniques with cryptool.
10. Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber-attack/vulnerability.

Activities suggested under PBL:

Sl. No.	Name of the activity	No. of hours	Evaluation Criteria
1	Assignment writing. Numerical based assignment is preferable.	5 assignments of 3h each. Total = 15h	Based on the assignment submitted.
2	Problem solving/Coding using C, C++, Python, SCILAB, MATLAB, MS-EXCEL or any other relevant software	5 small coding-based problems of 3h each. Total = 15h	Based on the coding solution submitted.
3	Technical Video based learning related to the subject	Duration of video = 5h Report preparation & Presentation = 10h Total = 15h	Report /presentation based on the video learning outcomes.

4	Discussion on research paper based on relevant subject	3 research paper = 15h	Summarize research paper and evaluation critical parameters
5	Poster/chart/power point preparation on technical topics	Duration = 10 h	Based on poster/chart preparation and presentation skills
6	Application/Software development	Duration = 15 h	Depending on the complexity of the
7	Group Discussion on emerging/trending technical topics based on subject	Duration = 1 h each	Based on performance in group discussion, technical depth, knowledge etc.
8	Seminar / Presentation	Duration for study and preparation=5h Report writing=3h Presentation=2h Total=10h	Topic can be selected technical content beyond syllabus
9	Real world case studies-based learning	Duration of data collection/study = 5h Report preparation = 10h Total = 15h	Based on in-depth study, technical depth, data collected, fact finding, etc.
10	Working/non-working model on technical topics	Working = 12 h Non- working = 8 h	Based on inter department/external evaluation
11	Self-learning on-line course	Minimum duration of the course should be 15h.	Examination based assessment at the end of course. Based on the certificate produced.
12	Complex problem solving	Maximum 3 problem. Study of the problem and solution finding, Total = 15h	Based on the depth of the solution submitted.
13	Industry/Research laboratory visit	Visit = 5h, Report preparation = 5h Total = 10h	Based on report submitted. Report should contain observations and calculations based on industry/ lab data.
14	Videos on Industrial safety aspects based on subject	Duration of video = 5h Report preparation = 5h Total = 10h	Based on quiz/report submitted
15	Industrial exposure for 2-3 days to observe and provide tentative solutions on society/environment /health/any other issue	Duration = 15 h for industrial exposure Problem identification and tentative solution = 10 h Total = 20 h	Based on evaluation of critical problems and solutions

Note:

- All the suggested activity should be related to the subject.
- Min 3 activities must be carried out as per the availability of faculties and students.
- The number of hours is suggestive. Faculty can sub-divide the number of hours based on the activity. However, total number of hours is fixed.
- Rubrics for the evaluation can be prepared by the faculty.
- All records pertaining to the evaluation and assessment of self-learning activities must be properly maintained and preserved at the institute level. These records should be made available to the university upon request.
- Institutes are encouraged to utilize digital platforms, such as Microsoft Teams, for effective record-keeping and to ensure transparency in the evaluation and assessment of self-learning activities.

* * * * * * *