GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Minor/Hons. Degree

Level: UG

Branch: Minor/Hons. Cyber Security

Subject Code: BE050AH011

Subject Name: Data Encryption

w. e. f. Academic Year:	2025-26
Semester:	5
Category of the Course:	Core Courses

Prerequisite:	Linear Algebra, Computer Networks
Rationale:	To prevent unauthorized users from accessing your precious data one of the ways is Data encryption. On the other hand, compressing data can save storage capacity, speed up file transfer, and decrease costs for storage hardware and network bandwidth. This course focus on various encryption techniques for securing data. The subject also covers various compression methods to decrease the file size.

Course Outcome:

After Completion of the Course, Student will able to:

No	Course Outcomes	% of Weightage
01	To analyze symmetric key and asymmetric key cryptography.	15
02	To learn DES, AES, RSA and other cryptographic algorithms.	25
03	To understand key distribution and communication model.	20
04	To study various models for data compression.	18
05	To Study Vulnerabilities in system, Network, Encryption in Cloud Computing and AI in Encryption with recent trends in encryption.	22

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)	
60	30	00	60	150	05	70	00	00	30	50	150

Course Content:

Unit No.	Content	No. of Hours	% of Weightage
1	**Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attack		20

	Encryption Techniques: Plaintext, Cipher text, Substitution & Transportation techniques, Encryption & Decryption, Types of attacks, Key range & size.	11	
2	**Symmetric & Asymmetric Key Cryptography:** Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.	9	12
3	**Case Studies of Cryptography:** Denial of service attacks, IP spoofing attacks, Conventional Encryption and Message Confidentiality, Conventional Encryption Algorithms, Key Distribution. **Public Key Cryptography and Message Authentication:** Approaches to message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key management, Firewall.	12	20
4	**Introduction Data Compression:** Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification. **Methods of Data Compression:** Data Compression—Loss less & Lossy	11	19
5	**Vulnerabilities** : Systems Vulnerability Scanning Overview of vulnerability scanning, Open Port, Traffic Probe, Vulnerability Probe, Vulnerability Examples, Metasploit. 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. **Encryption in Cloud**: Overview, advantages of cloud cryptography & disadvantages of cloud cryptography, key points related to cloud cryptography. Algorithms in cloud cryptography. **AI Enhanced Encryption:** AI Enabled and enhanced Encryption.	11	19
6	Recent trends in encryption and data compression techniques.	6	10
	Total	**60**	**100**

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
30	30	15	20	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. Cryptography and Network Security, Mohammad Ajmad, John Wiley & Sons.
2. Cryptography and Network Security by Atul Kahate, TMH.
3. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons
4. Cryptography and Network Security by B.Forouzan, McGraw-Hill.
5. The Data Compression Book by Nelson, BPB.

Suggested Course Practical List: If any

1. Write a program to perform encryption and decryption using Data Encryption Standard (DES).
2. Write a program to perform encryption and decryption using Advance Encryption Standard (AES).
3. Write a program to perform encryption and decryption using IDEA.
4. Implement RSA algorithm.
5. Perform packet tracing using Wireshark.
6. Study and prepare comparative analysis of SHA-1 and MD5.
7. Prepare case study on Digital Signature.
8. Web application testing using DVWA.
9. Prepare case study on Encryption in Cloud.
10. Prepare case study on Encryption and AI.

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.

* * * * * * *