GUJARAT TECHNOLOGICAL UNIVERSITY

Minor Degree: Cyber Security
Subject Code: 114AH01
Semester – IV
Subject Name: Information Theory for Cyber Security

Prerequisite: Computer Networks, Probability Theory

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.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
3	0	2	4	70	0	30	0	100

Content:

Unit No	Course Content	No of Hours
1	Shannon's foundation of Information theory, Random variables, Probability distribution factors, Uncertainty/entropy information measures, Leakage, Quantifying Leakage and Partitions, Lower bounds on key size: secrecy, authentication and secret sharing. provable security, computationally secure, symmetric cipher.	8
2	Secrecy, Authentication, Secret sharing, Optimistic results on perfect secrecy, Secret key agreement, Unconditional Security, Quantum Cryptography, Randomized Ciphers, Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques.	8
3	Information-theoretic security and cryptography, basic introduction to Diffie-Hellman, AES, and side-channel attacks.	8
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.	10
5	Digital and network forensics, Public Key Infrastructure, Lightweight cryptography, Elliptic Curve Cryptography and applications.	8
	Total Hrs.	**42**

Suggested Specification table (Theory):

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

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

GUJARAT TECHNOLOGICAL UNIVERSITY

Minor Degree: Cyber Security
Subject Code: 114AH01

Reference 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.

Course Outcomes: Upon completion of this course students should be able to:

No	Course Outcomes	% weightage
01	To introduce the principles and applications of information theory.	70%
02	To justify how information is measured in terms of probability and entropy.	15%
03	To learn coding schemes, including error correcting codes.	15%

List of Practical:

1. Implement Caesar cipher encryption-decryption.
2. Implement Monoalphabetic cipher encryption-decryption.
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.