GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering

Level: UG

Branch: Computer Science and Engineering (Data Science)

Course / Subject Code: 3164603

Course / Subject Name: Information Security

w. e. f. Academic Year:	A.Y. 2022-23
Semester:	6
Category of the Course:	Open Elective

Prerequisite:	Mathematical concepts: Random numbers, Number theory, finite fields, Computer network
Rationale:	The use of the Internet for various purpose including social, business, communication and other day to day activities has been in common place. The information exchanged through Internet plays 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 of Computer Engineering. The subject covers various important topics concern to information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies. The subject also covers the applications of all of these in real life applications.

Course Outcomes:

After Completion of the Course, Student will able to:

No	Course Outcomes	RBT Level
1	Explore the basic principles of the symmetric cryptography and techniques with their strengths and weaknesses from perspective of cryptanalysis	
2	Implement and analyze various symmetric key cryptography algorithms and their application in different context	
3	Compare public key cryptography with private key cryptography and Implement various asymmetric key cryptography algorithms	
4	Explore the concept of hashing and implement various hashing algorithms for message integrity.	

**Revised Bloom's Taxonomy (RBT)*

Teaching and Examination Scheme:

GUJARAT TECHNOLOGICAL UNIVERSITY

Program Name: Bachelor of Engineering

Level: UG

Branch: Computer Science and Engineering (Data Science)

Course / Subject Code: 3164603

Course / Subject Name: Information Security

Teaching Scheme (in Hours)			Total Credits L+T+ (PR/2)	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial / Practical		
L	T	PR	C	ESE (E)	PA / CA (M)	PA/CA (I)	ESE (V)	
2	0	2	3	70	30	20	30	150

Course Content:

Sr. No.	Course Content	No. of Hours	% of Weightage
1	Introduction & Classical Encryption Techniques : Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Symmetric cipher Model, Classical encryption techniques: substitution techniques, transposition techniques, steganography).- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis	7	30
2	Block Ciphers & Symmetric Key Cryptography, Data Encryption standard (DES) with example, strength of DES, AES with structure, its transformation functions, key expansion, example and implementation	5	20
3	Block Cipher Operations : Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	3	10
4	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security	4	20
5	Application of Cryptographic Hash Functions, Simple hash functions, its requirements and security, Secure Hash Algorithm (SHA)	2	5
6	Requirements and security of Message Authentication Codes , MACs based on Hash Functions, MACs based on Block Ciphers	2	5
7	Digital Signature, its properties, requirements, NIST digital Signature algorithm	3	10

Suggested Specification Table with Marks (Theory):

Distribution of Theory Marks (in %)					
R Level	U Level	A Level	N Level	E Level	C Level
30	30	22	10	10	-

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

Text books & Reference books:

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson.

2. Security In Computing By Pfleeger and Pfleeger , Pearson Education.

3. Cryptography& Network Security, Forouzan, Mukhopadhyay, McGrawHill.

4. Cryptography and Network Security Atul Kahate, TMH.

5. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India. 6. Information Systems Security, Godbole, Wiley-India.

Suggested Course Practical List: (List can be change according to Latest Development)

1. At least 15 practical using different encryption algorithms

* * * * * * *