GUJARAT TECHNOLOGICAL UNIVERSITY

BACHELOR OF ENGINEERING SYLLABUS

Subject Code : 3164204

Subject Name : Data Security

WEF Academic Year :	2020-21
Semester :	6
Category of the Course :	Professional Elective - II

Prerequisite : Basic mathematical knowledge

Rationale :

The objective of the data security course is to provide students with a comprehensive understanding of the various techniques and technologies used to protect sensitive information and ensure the confidentiality, integrity, and availability of data. The course covers mathematical foundations, cryptography, data encryption and decryption, data protection techniques and emerging trends in data security. The course aims to equip students with the knowledge and skills required to design and implement secure systems, evaluate security risks, and respond to security incidents. The course emphasizes hands-on experience through practical exercises and projects to provide students with the opportunity to apply their knowledge in real-world scenarios

Course Scheme :

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Tutorial/ Practical		
L	T	P	C	University exams (ESE)	Progressive Assessment (PA)	External Practical /viva Exam(ESE)	Internal evaluation Practical /viva Exam(PA)	
3	0	2	4	70	30	30	20	150

Course Content :

Unit No.	Content	No. of Hours	Weightage (%)
1	Introduction – Security services, security mechanisms Finite fields – group, ring, fields, modular arithmetic, The Euclidean algorithm	**3**	**5**
2	Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques	**4**	**10**
3	Stream ciphers and block ciphers, Block Cipher structure, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES with structure, its transformation functions, key expansion, example and implementation	**5**	**10**

4	Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	**5**	**10**
5	Public Key Cryptosystems with Applications, Requirements and Cryptanalysis, RSA algorithm, its computational aspects and security, Diffie-Hillman Key Exchange algorithm, Man-in-Middle attack	**7**	**15**
6	Cryptographic Hash Functions, their applications, Simple hash functions, its requirements and security, Hash functions based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	**5**	**10**
7	Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers	**4**	**10**
8	Digital Signature, its properties, requirements and security, various digital signature schemes (Elgamal and Schnorr), NIST digital Signature algorithm	**4**	**10**
9	Key management and distribution, symmetric key distribution using symmetric and asymmetric encryptions, distribution of public keys, X.509 certificates, Public key infrastructure. Remote user authentication with symmetric and asymmetric encryption, Kerberos	**7**	**15**
10	Case Studies and Projects A. Case Studies - Real-life Data Security incidents - Analysis of Data Security incidents B. Projects - Hands-on implementation of Data Security techniques - Group or individual projects on Data Security topics	**4**	**5**
	Total Hours :	**48**	**100**

Textbook :

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Information Security Principles and Practice By Mark Stamp, Willy India Edition
3. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGrawHill

Reference Books :

1. Cryptography and Network Security Atul Kahate, TMHCryptography and Network Security Atul Kahate, TMH
2. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
3. Information Systems Security, Godbole, Wiley-India

Course Outcomes :

No.	Course Outcomes	RBT Level*
1	Define terms related to cryptography, hashing, message authentication code, digital signature	RM
2	Analyze the principles and techniques of cryptography, such as symmetric and asymmetric encryption, digital signatures, and hash functions, and compare their strengths and weaknesses	UN
3	Demonstrate the generation of keys and execution of symmetric and public key algorithms from given data.	AP
4	Evaluate various data protection techniques, such as access control, data backup and recovery, and firewalls, and assess their effectiveness in securing data.	EL
5	Apply the concepts of data security to implement and create case study based project.	CR

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List :

Bellow is the suggested practical list. Extra practical can be added as per the requirements.

1	Implement Play fair cipher. The plaintext is paired in two characters. Discuss the advantage of poly alphabetic cipher over mono alphabetic cipher. Key = MONARCHY Plaintext = ar mu hs ea Cipher text = RM CM BP IM
2	Implement Ceasar and Hill cipher. Both are substitution cipher. Analyze the strength of the cipher in terms of brute force attack and cryptanalysis attack. Suggest one way to improve and strengthen the cipher and analyze with respect to cryptanalysis attack. Ceasar cipher - You are given plaintext Hello, Welcome. The key used is 3. How Ceasar cipher will work? Test case : A B C D E F Hill Cipher - Key K = 17 17 5 21 18 21 2 2 19 Plaintext = pay Cipher text = RRL

3	Implement Euclid algorithm to find GCD. GCD(16,12) = 4 GCD(12,4) = 0 Then 4 is the GCD(16,12)
4	Demonstrate how the RSA algorithm can be used to generate a public key and a private key for encrypting and decrypting messages, as well as for generating digital signatures.
5	Write a program or a function that performs the encryption and decryption operations using the AES algorithm.
6	Implement the SHA algorithm Write a program or a function that performs the following steps : Accept a message as input. Divide the message into blocks. Apply a series of logical operations, including bitwise operations and modular arithmetic, to each block to obtain a fixed-length output, referred to as the hash value or message digest

List of Laboratory/Learning Resources Required :

1. Software: cryptool (www.cryptool.org)
2. Software: Wireshark (www.wireshark.org)
3. http://www.cryptix.org/
4. http://www.cryptocd.org/
5. http://www.cryptopp.com/

Other Resources/MOOCs :

1. https://nptel.ac.in/
2. https://www.coursera.org/

* * * * * * *