Course Name	CRYPTOGRAPHY & DATA SECURITY		Course Code	ITEC-332		
Credit Hours	3		Contact Hours	Lecture	Lab	Total
				2	2	4
Offered as	☐ University Requirement ☐ College Requirement ☒ Program Requirement ☒ Core ☐ Elective ☒ ITEC ☐ COMP ☐ CNET					
Level	6		Prerequisite	ITEC331		

Course Description:

This course provides an insight into the fundamental ideas about cryptography, and discusses various security trends, services, and several types of attacks on network security. Also, this course elucidates the conventional encryption model, substitution, and transposition techniques, which are useful to learn about modern ciphers. It concentrates on Data Encryption Standard (DES) and presents the strength of DES and its different modes of operation. It discusses secure block cipher and stream cipher techniques with Double DES and Triple DES principles. Moreover, it outlines the structure of AES and its working principles. Also, it explores public key cryptography with asymmetric key algorithm RSA. It deals with key management and key distribution and provides a proper explanation of the Diffie–Hellman, and Elgamal key exchange algorithm. It also provides details about elliptic curve cryptography. It focuses on authentication techniques that prevent misuse of resources. Finally, it describes about message authentication code, standard hash functions like MD hash family, and SHA. expounds on the use of various digital signature schemes.

After successfully completing this course, students will be able to:

- Explain the fundamental concepts of cryptography and data security.
- Outline the concepts related to substitution, and transposition techniques.
- Identify various modes of operation for DES.
- Compare block and stream ciphers.
- Implement public key cryptosystems, elliptic curve cryptography, hash functions, and digital signature schemes.
- Recognize the ethical dilemmas and legal issues related to cryptography and data security.

Assessment Methods	☒ Assignment-1	10%	☒ Mid Exam	15%	☒ Mini Project	15%
			☒ Lab Exam	20%	☒ Final Exam	40%

Textbook:

- William Stallings, ”Cryptography and Network Security: Principles and Practice”, Pearson Education, 8th Global Edition, 2023, ISBN-13: 9781292437484.
- Ajay Kumar, “Cryptography and Network Security”, 1st Edition, Pearson Education, 2018, ISBN-13: 9789332578814.

References:

- Jonathan Katz,” Introduction To Modern Cryptography”, CRC Press/Taylor & Francis Group, 3rd Edition, 2021, ISBN-13: 9781351133005.
- Bhushan Trivedi, “Cryptography and Network Security”, BPB Publications, 1st Edition, 2022, ISBN-13: 9789389328660.