Course Name: Cryptography & Data Security **Course Code: ITEC332**

General Information						
Course Code	ITEC-332	**Level/Year**	$6^{th}/3^{rd}$	**Required (R) / Selected Elective (SE)**		R
Credit Hours	Theory	2	**Lab**	1	**Total**	3
Prerequisites	ITEC331	**Course Coordinator**		Dr. Haitham Elhadi		
Corequisites	-	**Track Leader**		Dr. Rahama Salman		

Course Description

This course provides an insight into the fundamental ideas about cryptography, and discusses various security trends, the ethical dilemmas and legal issues related to cryptography and data security, 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 algorithms. It also provides details about elliptic curve cryptography. It focuses on authentication techniques that prevent misuse of resources. Finally, it describes message authentication code, standard hash functions like MD hash family, and SHA. expounds on the use of various digital signature schemes.

Course Objectives : On completion of the course, the student will be able to:

- Understand 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.

Course Contents

List of Topics	Weeks
UNIT 1: Introduction to Cryptography and Data Security	1,2,3
UNIT 2: Block and Stream Ciphers	4, 5, 6
UNIT 3: Advanced Encryption Standard	7, 8, 9
UNIT 4: Public Key Cryptosystem, and Key Management	10, 11, 12
UNIT 5: Authentication Techniques, Hash Functions, and Digital Signature	13, 14, 15

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.

Reference Materials

- 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.

Course Learning Outcomes

CLO	Description	Mapped PI
CLO#01	**Define** the fundamental concepts of cryptography and data security.	PI 1.1
CLO#02	**Explain** the concepts of security threats and their defenses, security services, emerging security trends, various substitution methods, and key management schemes.	PI 1.2
CLO#03	**Identify** different types of passive and active security attacks, transposition methods, AES, and RC4 encryption and decryption steps.	PI 1.3
CLO#04	**Compare** various block and stream ciphers, public key encryption schemes, key exchange methods, authentication methods, hash functions, and digital signature schemes.	PI 2.2
CLO#05	**Apply** and evaluate substitution and transposition ciphers, public key encryption schemes, hash functions, and key exchange methods using elliptic curve cryptography.	PI 2.3 PI 2.4 PI 6.3
CLO#06	**Identify** and analyze security requirements for computing solutions, with a focus on cryptography and data protection.	PI 6.1

CLO-PI-SO Mapping

	SO-1	SO-2	SO-3	SO-4	SO-5	SO-6
CLO#01	PI 1.1	-	-	-	-	-
CLO#02	PI 1.2	-	-	-	-	-
CLO#03	PI 1.3	-	-	-	-	-
CLO#04	-	PI 2.2	-	-	-	-
CLO#05	-	PI 2.3 PI 2.4	-	-	-	PI 6.3
CLO#06	-	-	-	-	-	PI 6.1