

Branch Name:	Signal Processing and Communication
Program Code:	ET214
Course Name:	Cryptography and Wireless Security
Course Code:	2ET2140402T
Pre-requisite Subject	Fundamentals of Networking

Course Objective:

1. To study the properties of the three-dimensional world from digital images.
2. To study the Problems in this field include identifying the 3D shape of an environment, determining how things are moving, and recognizing familiar people and objects, all through analysis of images and video.
3. To study the introduction to computer vision, including such topics as feature detection, motion estimation, image mosaics, 3D shape reconstruction, and object recognition.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Sr. No	Topic	Total Hours	Weight (%)
1	Introduction: Security Goals, Security Attacks, Services and Mechanism, Techniques – Cryptography and Steganography	03	10
2	Symmetric Key Ciphers: Categories of Traditional Ciphers, Modern Block Ciphers, Modern Stream Ciphers	07	15
3	Data Encryption Standards and Advance Encryption Standard: DES structure and Analysis, Security of DES, AES Origins, AES Structure and Analysis, AES Round Functions and Transformation, AES Key Expansion and Implementation	10	25
4	Block Ciphers and Asymmetric Key Cryptography: Use of Modern Block Ciphers, RSA Cryptosystem, Elgamal Cryptosystem, Elliptical curve Cryptosystem, Message Integrity, Message Authentication	11	30
5	Cryptographic Hash Function and Digital Signature : Introduction, SHA-512, Wirlpool, Digital Signatures, Attacks on Digital Signature, Digital Signature Scheme	08	20

List of Text Book:

1. Cryptography and Network Security, Behrouz A. Forouzan, Tata Mc-Graw Hill Publications.

List of Reference Books:

1. Introduction to Cryptography with coding theory, Wade Trappe, Lawrence C Washington, 2nd ed, Pearson.
2. Cryptography and Network security Principles and Practices, William Stallings, Pearson/PHI, 4th ed, 2006.

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	To Understand Symmetric Cipher Model and Substitution Ciphers	1 Remembering 2 Understanding
CLO2	To Understand Transposition Ciphers and Block Cipher Principles	2 Understanding
CLO3	To Understand DES and Be able to apply Block Cipher Design Principles and To Understand AES Be able to conduct basic Block Cipher Operations	2 Understanding
CLO4	To Understand Principles of Public Key Cryptosystems and Understand the RSA Algorithm	2 Understanding 3 Applying
CLO5	To Be able to apply Hash Functions and Be able to apply Message, Authentication Codes	2 Understanding 4 Analyze
CLO6	To Understand and apply Digital Signatures	2 Understanding 6 Create

Mapping of CLOs with POs & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1					L	M						H	H	M	L	
CLO2		H	M	M	L					L		H		M	L	
CLO3		M	H		L									H		L
CLO4		M	H		L			L					L		M	H
CLO5	H	M	H		L				L			H	L		M	H
CLO6	H	M	H		L							M	L		M	H

H: High, M: Medium, L: Low