School:		**School of Engineering and technology**
Department		**Department of Computer Science and Engineering**
Program:		**M. Tech**
Branch:		**M. Tech. (CSE) Networking and Cyber Security**
1	Course Code	CSE632
2	Course Title	Advanced Network Security
3	Credits	3
4	Contact Hours (L-T-P)	3-0-0
	Course Status	Elective
	Course Objective	The objective of this course is to provide an apprehension to the threats and issues of Network Security and cryptography and about key security requirements of networks, symmetric and asymmetric ciphers and application through Algorithms.
6	Course Outcomes	On successful completion of this module students will be able to: CO1: Identify the key security requirements of confidentiality, integrity, and availability, security architecture for OSI, categories of computer and network assets, fundamental security design principles, and cryptography standards CO2: Interpret knowledge of symmetric and asymmetric ciphers, classical encryption techniques, block ciphers and data encryption standard, and public key cryptography. CO3: Categorize cryptographic data integrity algorithms, cryptographic, hash function, message authentication codes, digital signatures and user authentication. CO4: Extend network access control and cloud security, transport level security, wireless network security, electronic mail security and IP security. CO5 Organize the security measures of a network in Informational resources.

		CO6 Evaluate the principles of Network Security in real time applications	
7	Course Description	This course will provide a systematic approach of both the principles and practice of Advanced concepts in network security. It covers the basic issues to be addressed by a network security capability, and explored by providing a tutorial and survey of cryptography and network security technology.	
8	Outline syllabus		CO Mapping
	Unit 1	**Basic Concept of Network Security**	
	A	Network Security Model, OSI Security Architecture, Goals of network security and standards.	CO1,CO6
	B	Basic concepts of cryptography	CO1, CO2, CO4
	C	Introduction to IT-Security in Open system, threats to security, security requirements and how it works.	CO1, CO2,CO6
	Unit 2	**Network Security Threats and Issues**	
	A	Protocol Vulnerabilities: DoS and DDoS, SYN Flooding, Session Hijacking, ARP Spoofing, Attack on DNS.	CO1, CO2,CO6
	B	Wireless LAN: Frame spoofing, Violating MAC; Software Vulnerabilities: Phishing Attack, Buffer Overflow, Cross-site Scripting	CO2,CO4
	C	SQL Injection; Virus, Worm, Malware, Botnets; Eavesdropping, Password Snooping and IP Masquerade	CO2,CO4
	Unit 3	**Security at Network Level**	
	A	Authentication: password-based, certificate-based, Centralized; Kerbos, Biometrics., SSL.	CO2,CO3,CO6
	B	IP Security, IKE, Virtual Private Network.	CO1,CO2,CO6
	C	Open SSL, Wireless LAN Security: WEP,	CO4,CO2,CO5

		TKIP, CCMP.			
	Unit 4	**Firewall Introduction to ACL**			
	A	Introduction to Firewall, Firewall Functionalities, Types of Firewalls.			CO1,CO2,CO3
	B	Packet Filtering, Reverse Proxy, Stateful Firewalls, limitation of Stateful FireWalls.			CO1,CO2,CO3,CO6
	C	Application Firewalls, Circuit Firewalls, CHECK Point, CISCO PIX, CISCO firewalls case study.			CO1,CO2,CO3
	Unit 5	**Security and Network Applications**			
	A	Electronic Payment: Payment types, SET, Chip Card Transaction.			CO2,CO3,CO4
	B	Mobile Payments; Electronic Mail Security, Web Security: SSL and TLS			CO1,CO3,CO4,CO5
	C	Web Service Security: Token Type, XML Encryption, XML Signatures, SAML; Intrusion detection and prevention systems; honey pots.			CO2,CO3,CO4,CO6
	Mode of examination	Theory			
	Weightage Distribution	CA	MTE	ETE	
		25	25%	50%	
	Text book/s*	1. Bernard Menezes, “Network Security and Cryptography”,Cengage Learning.			
	Other References	1. Raymond R. Panko,“Corporate Computer and Network Security”, Pearson Education. 2. Willam Stallings, “Cryptography and Network Security”, Pearson Education. 3. Internet as a resource for references			

CO and PO Mapping

S. No.	Course Outcome	Program Outcomes (PO) & Program Specific Outcomes (PSO)
1.	CO1: Identify the key security requirements of confidentiality, integrity, and availability, security architecture for OSI, categories of computer and network assets, fundamental security design principles, and cryptography standards	PO1,PO4 PSO
2.	CO2: Interpret knowledge of symmetric and asymmetric ciphers, classical encryption techniques, block ciphers and data encryption standard, and public key cryptography.	PO1, PO2,PO3,PSO
3.	CO3: Categorize cryptographic data integrity algorithms, cryptographic, hash function, message authentication codes, digital signatures and user authentication.	PO2, PO3,PSO
4.	CO4: Extend network access control and cloud security, transport level security, wireless network security, electronic mail security and IP security.	PO2, PO4,PO6,PSO
5.	CO5: Organize the security measures of a network in Informational resources.	PO1, PO5, PO6,PO7, PSO
6.	CO6: Evaluate the principles of Network Security in real time applications	PO4, PO5,PO8, PSO

PO and PSO mapping with level of strength for Course Name Advanced Network Security (Course Code CSE632)

Course Code_ Course Name	CO's	PO 1	PO2	PO 3	PO4	PO5	PO6	PO7	PO8	PSO
CSE632_Advanced Network Security	CO1	2	-		2	-	-	-	-	2
	CO2	2	2	2	-	-	-	-	-	2
	CO3	-	2	2	-	-	-	-	-	2
	CO4	-	2	-	2	-	2	-	-	2
	CO5	2	-	-	-	2	2	2	-	2
	CO6	-	-	-	2	2	-	-	2	2

‘

Average of non-zeros entry in following table (should be auto calculated).

Course Code	Course Name	PO 1	PO2	PO 3	PO 4	PO5	PO6	PO7	PO8	PSO
CSE632	Advanced Network Security	2	2	2	2	2	2	2	2	2

Strength of Correlation

1. Addressed to***Slight (Low=1)*** ***extent*** ***2.*** Addressed to***Moderate (Medium=2)*** ***extent***

3. Addressed to***Substantial (High=3)*** ***extent***