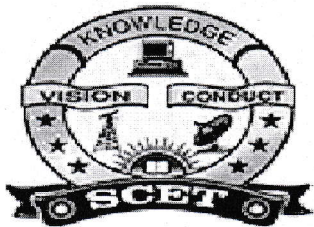# SWARNANDHRA
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Accredited by National Board of Accreditation, AICTE, New Delhi,Accredited by
NAAC with "A" Grade – 3.32 CGPA,Recognized under 2(f) & 12(B) of UGC Act 1956,
Approved by AICTE, New Delhi,Permanent Affiliation to JNTUK, Kakinada
Seetharampuram, W.G.DT., Narsapur-534280, (Andhra Pradesh)

DEPARTMENT OF INFORMATION TECHNOLOGY
TEACHING PLAN

Course Code	Course Title	Semester	Branch	Contact Periods /Week	Academic Year	Date of commencement of Semester
16IT7T02	CRYPTOGRAPHY AND NETWORK SECURITY	VII	IT	6	2021-2022	04-10-2021

COURSE OUTCOMES

1	Explain the basic knowledge of different types of Security attacks.
2	Distinguish different modern encryption Algorithms.
3	Understand mathematical foundation required for various cryptographic algorithms.
4	Compare different Authentication Mechanisms.
5	Justify latest techniques used in different Security aspects (e.g. network security, web security etc.)

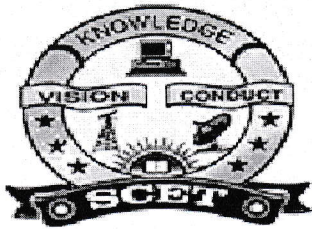| UNIT	Out Comes / Bloom's Level	Topics No.	Topics/ Activity	Text Book/ Reference	Contact Hour	Delivery Method
I	CO – 1	1.1	**Introduction:** Security Attacks	T2	1	Chalk & Board Power point presentation Assignment Test
		1.2	Security Services	T2	1	
		1.3	Security Mechanisms	T2	1	
		1.4	Model for Network Security	T2	1	
		1.5	**Basics of Cryptography**	T2	1	
		1.6	Symmetric Cipher Model	T2,T1	1	
		1.7	Substitution Techniques	T2,T1	1	
		1.8	Transportation Techniques	T2,T1	1	
		1.9	Stegnography	T2,T1	1	
			Total		09	
II	CO – 2	2.1	**Secret Key Cryptography**	T1	1	Chalk & Board Power point presentation Assignment
		2.2	Data Encryption Standard(DES)	T1	1	
		2.3	Strength of DES	T1	1	
		2.4	Block Cipher Design Principles	T1	1	
		2.5	Modes of Operations	T1	1	
		2.6	Triple DES	T1	1	
		2.7	Blowfish Algorithm	T1	1	
		2.8	Blowfish Algorithm with example	T1	1	

SWARNANDHRA
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Accredited by National Board of Accreditation, AICTE, New Delhi, Accredited by NAAC with "A" Grade – 3.32 CGPA, Recognized under 2(f) & 12(B) of UGC Act 1956, Approved by AICTE, New Delhi, Permanent Affiliation to JNTUK, Kakinada Seetharampuram, W.G.DT., Narsapur-534280, (Andhra Pradesh)

		2.9	AES Algorithm	T1	1	Test
		2.10	An example for AES Algorithm	T1	1	
Course beyond syllabus		2.11	IDEA Encryption Algorithm	T1	1	
				Total	11	
III	CO - 3	3.1	**Number Theory:**	T1,R1	1	Chalk & Board

Power point presentation

Assignment

Test |
		3.2	Prime and Relatively Prime Numbers	T1,R1	1	
		3.3	Modular Arithmetic	T1,R1	1	
		3.4	Modular Arithmetic with an example	T1,R1	1	
		3.5	Fermat's Theorem	T1,R1	1	
		3.6	Euler's Theorem	T1,R1	1	
		3.7	Chinese Remainder Theorem	T1,R1	1	
		3.8	Chinese Remainder Theorem with example	T1,R1	1	
		3.9	Discrete Logarithms	T1,R1	1	
		3.10	Discrete Logarithms with an example	T1,R1	1	
				Total	10	
IV	CO – 4	4.1	**Public Key Cryptography:**	T1,T2	1	Chalk & Board

Power point presentation

Assignment

Test |
		4.2	Principles of Public Key Cryptosystems	T1,T2	1	
		4.3	RSA Algorithm	T1,T2	1	
		4.4	RSA Algorithm with an example	T1,T2	1	
		4.5	Diffie-Hellman Key Exchange	T1,T2	1	
		4.6	Diffie-Hellman Key Exchange with example	T1,T2	1	
		4.7	Introduction to Elliptic Curve Cryptography	T1,T2	1	
		4.8	Introduction to Elliptic Curve Cryptography with an example	T1,T2	1	
Course beyond syllabus		4.9	Key Serialization	T1	1	
				Total	9	
V	CO – 5	5.1	**Cryptographic Hash Functions:** Applications of Cryptographic Hash Functions	T1	1	Chalk & Board

Power point presentation

Assignment |
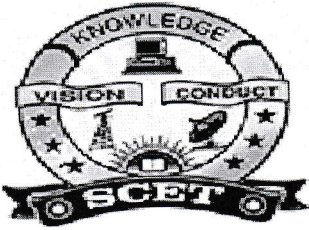| | | 5.2 | Secure Hash Algorithm | T1 | 1 | |
		5.3	Secure Hash Algorithm with example	T1	1	
		5.4	MD5	T1	1	
		5.5	Message Authentication Codes	T1	1	
		5.6	Message Authentication	T1	1	

SWARNANDHRA
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Accredited by National Board of Accreditation, AICTE, New Delhi, Accredited by
NAAC with "A" Grade – 3.32 CGPA, Recognized under 2(f) & 12(B) of UGC Act 1956,
Approved by AICTE, New Delhi, Permanent Affiliation to JNTUK, Kakinada
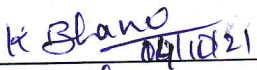Seetharampuram, W.G.DT., Narsapur-534280, (Andhra Pradesh)

			Requirements and Functions			Test
		5.7	Message Authentication Functions	T1	1	
		5.8	HMAC	T1	1	
		5.9	HMAC with an example	T1	1	
		5.10	Digital signatures	T1	1	
		5.11	Digital Signature Schemes	T1	1	
		5.12	Digital Signature Schemes with an example	T1	1	
		5.13	Authentication Protocols	T1	1	
		5.14	Authentication Protocols	T1	1	
		5.15	Digital Signature Standards	T1	1	
			Total		**15**	
VI	CO – 6	6.1	**Authentication Applications:**	T1,R1	1	Chalk & Board Power point presentation Assignment Test
		6.2	Kerberos, X.509 Authentication Service	T1,R1	1	
		6.3	Electronic Mail Security	T1,R1	1	
		6.4	Electronic Mail Security	T1,R1	1	
		6.5	Pretty Good Privacy (PGP)	T1,R1	1	
		6.6	Pretty Good Privacy (PGP)	T1,R1	1	
		6.7	S/MIME	T1,R1	1	
		6.8	S/MIME	T1,R1		
		6.9	**IP Security:**	T1,R1	1	
		6.10	IP Security architecture	T1,R1	1	
		6.11	Web Security	T1,R1	1	
		6.12	Intruders	T1,R1	1	
		6.13	Malicious Software	T1,R1	1	
		6.14	Firewalls	T1,R1	1	
			Total		**14**	
			CUMULATIVE PROPOSED PERIODS		**68**	

Text Books:

S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1	William Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Pearson Education, 2011.
2	Bernard Menezes, Network Security and Cryptography, Cengage Learning, 2011.
3	Behrouz A. Fourouzan and Debdeep Mukhopadhyay, Cryptography and Network, 2nd Edition, McGraw-Hill, 2010.

Reference Books:

S.No.	AUTHORS, BOOK TITLE, EDITION, PUBLISHER, YEAR OF PUBLICATION
1	Eric Maiwald Fundamentals of Network Security by (Dreamtech press)
2	Whitman, Thomson Principles of Information Security.
3	Buchmann, Springer Introduction to Cryptography.

Web Details:

SWARNANDHRA
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Accredited by National Board of Accreditation, AICTE, New Delhi, Accredited by
NAAC with "A" Grade – 3.32 CGPA, Recognized under 2(f) & 12(B) of UGC Act 1956,
Approved by AICTE, New Delhi, Permanent Affiliation to JNTUK, Kakinada
Seetharampuram, W.G.DT., Narsapur-534280, (Andhra Pradesh)

1	https://www.geeksforgeeks.org/cryptography-and-network-security-principles
2	https://www.tutorialspoint.com/cryptography
3	https://www.javatpoint.com/computer-network-security
4	https://en.wikipedia.org/wiki/Network_security

		Name	Signature with Date
i.	Faculty	Mr. K.Bhanu Chand	K Bhanu 04/10/21
ii.	Module Coordinator	Mr. K Raja	K. Raja
iii.	Programme Coordinator	Dr. RVVSV Prasad	RVSuprasad 4/10/21

Principal