DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE & Affiliated to Anna University, Chennai)
Re-Accredited by NAAC with 'A' Grade
Accredited by NBA for AERO, BME, CSE, ECE, EEE, IT & MECH.
PERAMBALUR-621212, TAMILNADU, INDIA.
Website: www.dsengg.ac.in

COURSE PLAN

Name of the Faculty				
Designation/Department	AP/IT			
Course Code/Name	**U20IT703/CRYPTOGRAPHY AND NETWORK SECURITY**			
Year/Section/Department	IV/A,B & C/IT			
Credits Details	L:3	T:0	P:0	C:3
Total Contact Hours Required	45			

Syllabus:

UNIT I INTRODUCTION	**9**
Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.	
UNIT II SYMMETRIC KEY CRYPTOGRAPHY	**9**
MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic-Euclids algorithm- Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis - Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard - RC4 – Key distribution	
UNIT III PUBLIC KEY CRYPTOGRAPHY	**9**
MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem - Chinese Remainder Theorem – Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange - ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.	
UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY	**9**
Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC– SHA –Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509	
UNIT V SECURITY PRACTICE AND SYSTEM SECURITY	**9**
Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.	

OBJECTIVES:

- To learn the concepts of number theory, cryptographic techniques.
- To understand integrity and authentication process.
- To familiarize various cyber threats, attacks, vulnerabilities, defensive mechanisms, security policies and practices.

Text Book:

1. William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
2. Cryptography and network security principles and practice, william-stallings-7th edition, 2006.

Reference Book:

R1: C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd
R2: Behrouz A.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
R3: Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall, ISBN 0-13-046019-2

Website:

W1: https://www.geeksforgeeks.org/cryptography-introduction
W2: https://www.tutorialspoint.com/cryptographIc network security/security key.html

Online Mode of Study (if Any):

- http://nptel.ac.in/courses/106105031/lecture by Dr. Debdeep Mukhopadhyay IIT Kharagpur
- https://www.coursera.org/learn/crypto#syllabus

Course Plan:

Topic Number	Topic	Reference Detail	Page Number	Mode of teaching	Number of Periods Required	Cumulative Period
UNIT I INTRODUCTION						
1	Security trends, Legal, Ethical and Professional Aspects of Security	T1	33-37	BB	1	1
2	Need for Security at Multiple levels, Security Policies	T1	40-45	PPT	1	2
3	Model of network security	T1	49-51	BB	1	3
4	Security attacks	T1	39-43	BB	1	4
5	Services and mechanisms	T1	47-49	BB	1	5
6	OSI security architecture	T1	31-54	BB	1	6
7	Classical encryption techniques: substitution techniques	T1	55-76	BB	1	7
8	Transposition techniques, steganography	T1	77-89	BB	1	8
9	Foundations of modern cryptography	W1	-	BB	1	9
Outcome of Unit I: C01: Describe the fundamentals of networks security, security architecture, threats and vulnerabilities.						

UNIT II SYMMETRIC KEY CRYPTOGRAPHY						
10	Mathematics Of Symmetric Key Cryptography: Algebraic structures	T1	125-129	PPT	1	10
11	Modular arithmetic	T1	132-136	PPT	1	11
12	Euclid's algorithm, Congruence and matrices	T1	128-139	PPT	1	12
13	Groups, Rings, Fields, Finite fields	T1	140-144	BB	1	13
14	SYMMETRIC KEY CIPHERS**:** SDES, Block cipher Principles of DES, Strength of DES	T1	112-134	BB	1	14
15	Differential and linear cryptanalysis, Block cipher design principles	W2	-	PPT	1	15
16	Block cipher mode of operation	T1	216-230	BB	1	16
17	Evaluation criteria for AES, Advanced Encryption Standard	T1	171-215	BB	1	17
18	RC4, Key distribution.	T1	258-261	BB	1	18
Outcome of Unit II: CO2: Discuss the mathematical support for both symmetric and asymmetric key cryptography.						
UNIT III PUBLIC KEY CRYPTOGRAPHY						
19	Mathematics Of Asymmetric Key Cryptography: Primes	T1	267-271	BB	1	19
20	Primality Testing , Factorization	T1	275-277	BB	1	20
21	Euler's totient function, Fermat's and Euler's Theorem	T1	280-283	PPT	1	21
22	Chinese Remainder Theorem	T1	287-289	PPT	1	22
23	Exponentiation and logarithm	T1	290-295	BB	1	23
24	Asymmetric Key Ciphers: RSA cryptosystem, Key distribution	T1	300-305	BB	1	24
25	Key management	T1	315-320	BB	1	25
26	Diffie Hellman key exchange, ElGamal cryptosystem	T1	321-325	BB	1	26
27	Elliptic curve arithmetic, Elliptic curve cryptography	T1	-	PPT	1	27
Outcome of Unit III: CO3: Make use of symmetric key cryptographic algorithms to perform cryptographic operations.						
UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY						
28	Authentication requirement	T1	386-389	PPT	1	28
29	Authentication function	T1	389-389	PPT	1	29
30	MAC	T1	390-396	BB	1	30
31	Hash function ,Security of hash function and MAC	T1	398-404	BB	1	31
32	SHA	T1	366-376	BB	1	32
33	Digital signature and authentication	T1	419-423	BB	1	33

	protocols, DSS					
34	Entity Authentication: Biometrics, Passwords, Challenge Response protocols	T1	445-447	BB	1	34
35	Authentication applications	T1	-	PPT	1	35
36	Kerberos, X.509	T1	459-463	BB	1	36
Outcome of Unit IV: CO4: Solve cryptographic operations using public key cryptographic algorithms.						
UNIT V SECURITY PRACTICE AND SYSTEM SECURITY						
37	Electronic Mail security	T1	591-592	BB	1	37
38	PGP	T1	592-610	BB	1	38
39	S/MIME	T1	611-62	BB	1	39
40	IP security	T1	639-650	BB	1	40
41	Web Security	T1	650-673	PPT	1	41
42	System Security: Intruders	T1	676-678	BB	1	42
43	Malicious software	T1	686-687	BB	1	43
44	Viruses	T1	690-695	PPT	1	44
45	Firewalls	T1	696-699	PPT	1	45
Outcome of Unit V: CO5: Apply the various Authentication schemes to simulate different applications. CO6: Explain various Security practices and System security standards.						

Course Outcome:

At the end of course:
Students should be able to do:

CO1: Describe the fundamentals of networks security, security architecture, threats and vulnerabilities (K2)
CO2: Discuss the mathematical support for both symmetric and asymmetric key cryptography (K2)
CO3: Make use of symmetric key cryptographic algorithms to perform cryptographic Operations (K3)
CO4: Solve cryptographic operations using public key cryptographic algorithms (K3)
CO5: Apply the various Authentication schemes to simulate different applications. (K3)
CO6: Explain various Security practices and System security standards (K2)

Course Outcome Vs Program Outcome Mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	1	-	-	-	-	-	-	-	-	-	3	2
CO2	2	1	1	-	-	-	-	-	-	-	-	-	3	2
CO3	3	2	2	1	-	-	-	-	-	-	-	-	2	3
CO4	3	2	2	1	-	-	-	-	-	-	-	-	2	3
CO5	3	2	2	1	-	-	-	-	-	-	-	-	2	3
CO6	2	1	1	-	-	-	-	-	-	-	-	-	2	2
AVG:	**2.5**	**1.5**	**1.5**	**1.0**	-	-	-	-	-	-	-	-	**2.0**	**2.0**

Content Beyond Syllabus/Gap identification:

- Security and Privacy in Mobile and Wireless Networking
- Computational Security Analysis

Internal Evaluation Components

Web portal	Assignment	Components	Topic Number with Topic / Unit Details	Relevance to CO
Web portal 1	--	Assessment – I (60)	Unit I and II	CO1 & CO2
	1	Assignment Handwritten (20)	1.Security attacks 6.OSI security architecture 7.Classical encryption techniques:substitution techniques	CO1
	2	Poster / PPT Presentation (20)	14.Symmetric ciphers**:** SDES, Block cipher Principles of DES, Strength of DES 16.Block cipher mode of operation	CO2
Web portal 2	--	Assessment – II (60)	Unit III and IV	CO3 & CO4
	3	Seminar (20)	22.Chinese Remainder Theorem 26.Diffie Hellman key exchange, ElGamal cryptosystem	CO3
	4	Case Study Report/ Mini Project/Model Making (20)	33.Digital signature and authentication protocols, DSS 36.Kerberos, X.509	CO4
Web portal 3	--	Model Exam (75)	Unit I to V	CO1 to CO6
	5	MCQ (15)	Unit I to V	CO1 to CO6
	--	Course Attendance (10)	--	--

Submission Details:

Phase 1(Before AT 1)	Phase 2 (Before AT 2)	Phase 3 (Before AT 3)
Assignment 1	Assignment 2	Assignment 3

Google Class Name: U20IT703/CRYPTOGRAPHY AND NETWORK SECURITY
Google Class Code: yk77ezx6

Prepared By **Verified By**

Approved By