NAGARJUNACOLLEGEOFENGINEERINGANDTECHNOLOGY

NBA Accredited * grade(AnISO9001 –2008CertifiedInstitution)
Affiliated to Visvesvaraya Technological University
(VTU)Recognized by Govt. of Karnataka & Approved by A.I.C.T.E. New Delhi

DEPARTMENT OF ELECTRONICS & COMMUNICATIONENGINEERING

COURSEPLAN

(Tobesubmittedbeforecommencementofsemester)

Course Name: Cryptography and Network Security	**CourseCode**:20HOE752
CourseCredits:3	**Semester:**7th
Course Teacher/s: Mr.MaheshM R	**AcademicYear:**2023-24
Lab. Instructors(if applicable):NA	**DateofCommencementofClass:**19.10.2023

SUBJECTDESCRIPTION:

This Course covers the fundamental principles and techniques of Cryptography and Network Security.ThemaintopicscoveredareIntroductiontoCryptography,Finite fields, Block ciphers, authentication and Hash functions and Web Security. Cryptography is an art of science using mathematics data is encrypted and decrypted. As such, its primary goal is to protect data and provide security from unauthorized access. The main outcomes of Cryptography and Network securityis to design and develop the private key and public key, authentication functions for applications in network security. The purpose of this course is to provide security for data using various cryptographic algorithm.

PREREQUISITES:

1. Basic Knowledge in Modulus, Fundamentals of Algorithms.

LECTUREPLAN:

Topic	TopicDetails	Numberof Lectures	Prediction	Unit/Chapter Reference	Percentage ofModule coverage
ModuleI	Introduction	1	**Week1**	T1 1.1	
	OSI security architecture,Services, mechanisms and attacks	2		T1 1.2,1.3,1.4,1.5	

Introduction Symmetric cipher	Modelfor network security.	3		T11.6	**20%**
	SymmetricCipher Model	4	**Week2**	T12.1	
	Substitution Techniques:Caesar Cipher ,Mono Alphabetic Cipher ,PlayfairCipher	5		T12.2	
	HillCipher	6		T12.2	
	PolyalphabeticCipher and One-Time Pad	7	**Week3**	T1 2.2	
	Transposition Techniques,Rotor Machines, Steganography	8		T1 2.3,2.4,2.5	
	CumulativeCoverage				**20%**
Module II Finitefields	Groups,Rings, Fields. Modular Arithmetic:Divisors.	9	**Week4**	T24.2	**20%**
	Propertiesofmodulo operator properties	10		T24.2	
	FindingGCD	11		T24.3	
	Modulararithmetic operations and properties	12	**Week5**	T24.3	
	Euclid'sAlgorithm, GreatestCommon Divisor (GCD)	13		T24.4	
	Finite Fields of the form GF (p): Finite fields of order p, findingmultiplicative inverse inGF(p).	14	**Week6**	T24.5	
	polynomial Arithmetic, polynomial Arithmeticwith coefficientsinZp.	15		T24.6	
	Polynomial Arithmetic:Ordinary Finding GCD. Finite fields of the form GF(2^n).	16		T2 4.7	
	CumulativeCoverage				**40%**
AAT1		17			

Module III **Blockcipher**	BlockCipher Principles	18	**Week7**	T13.1	**20%**
	SimplifiedDES	19		T13.2	
	Dataencryption standard (DES)	20	**Week8**	T13.3	
	StrengthofDES	21		T13.4,3.5	
	BlockCipher Design	22		T13.6	
	PrinciplesandBlock Cipher Modes of Operation	23	**Week9**	T13.6	
	EvaluationCriteria for Advanced EncryptionStandard	24		T15.1	
	TheAESCipher	25		T1 5.2	
	CumulativeCoverage				**60%**
Module IV **Blockciphers** **Authentication functions and hashfunctions**	PrinciplesofPublic-Key Cryptosystems	26	**Week10**	T1 9.1	**20%**
	TheRSAalgorithm	27		T19.2	
	KeyManagement	28	**Week11**	T19.2	
	Diffie-HellmanKey Exchange	29		T110.1	
	OverviewofElliptic curve Cryptography	30		T110.3	
	Hashfunctions	31	**Week12**	T1 11.1	
	Authentication functions	32		T1 12.2	
	Message authenticationcodes	33		T1 12.3	
	CumulativeCoverage				**80%**
AAT2		34			
Module V **WebSecurity**	Web Security Consideration	35	**Week13**	T116.1	
	Securitysocketlayer (SSL)	36		T1 16.2	
	Transportlayer Security(TLS)	37	**Week14**	T1 16.3	
	Secure Electronic Transactio n(SET)	38		T1 16.4	
	SET Participant	39		T1 16.4	

	s				
	Intruders	40	**Week15**	T1 18.1	
	IntrusionDetection.	41		T1 18.2	
	Revision	42			
	CumulativeCoverage				**100%**

TEXTBOOKSANDREFERENCEBOOKS:

Book Type	Code	Title &Author	PublicationInformation		
			Edition	**Publisher**	**Year**
Text Books	**T1**	"CryptographyandNetwork Security: PrinciplesandPractice",WilliamStallings	5th	Pearson Education	2011
Reference Books	**R1**	"CryptographyandNetworkSecurity", Behrouz Forouzan	33d	TataMcGraw-Hill	2007
	R2	"HandbookofAppliedCryptography" **A**lfredJ.Menezes,PaulC.Van OorschotandScottA.Vanston	4th	CRCPress	2001
	R3	"CryptographyAndnetwork Security",AtulKahate	2nd	TataMcGraw-Hill	2006

COURSEOUTCOMES:

Attheendofthecoursethestudentwillbeableto:

CO1	Explainthebasicconceptofclassicalencryptionusedfornetworksecurity.
CO2	Illustratethestructureofcryptographicalgorithmandtheirapplications.
CO3	Applythe conceptsofclassicalencryptiontechniquestoexistingstandardalgorithms.
CO4	Evaluatethesignificanceofcryptographicalgorithmsandtheirapplicationsinnetworksecurity
CO5	Designanddeveloptheprivatekeyandpublickey,authenticationfunctionsfor applicationsin network security.

CO-POMAPPING:

POS	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
COs												
C405.1	3	3	3	2	2	1	1			2	1	
C405.2	3	3	3	3	2	1				2	2	
C405.3	3	3	3	2	2	1				2	2	
C405.4	3	3	2	2	2	1				2	2	1
C405.5	3	3	2	3	2	1	1			2	2	1

EVALUATIONSCHEME:

Component		**Weightage(%)**		
CIE’s	CIE15thweek	40	80	SumofBesttwooutofthreeCIE
	CIE210thweek	40		
	CIE315thweek	40		
AAT’s	AAT1(Quiz)	10	20	SumoftwoAATs
	AAT2(Surprisetest)	10		
ContinuousInternalEvaluationTotalMarks:100.Reducedto50Marks **TheminimumpassingmarkfortheCIEis40%ofthemaximummarks(20 marksoutof 50)**				
SemesterEndExamination(SEE)TotalMarks:100.Reducedto50Marks **Theminimumpassing markfortheSEEis40%ofthemaximummarks(20marksoutof 50)**				

SignatureoftheCourseCo-Ordinator **SignatureoftheHOD**

Date:18.10.2023

Note:

1. TheCourseplanisanattempttoensure**continuousimprovement**intheTLPofthecourse.
2. TheproposedCoursePlanissubmittedto**DAC**beforethecommencementofthesemester.
3. Attheendofthesemester,thefacultyshallsubmitthe **actualimplementedplan**.
4. CalendarofEventsincluded.