Department	Computer Science & Engineering			
Course Name	Cryptography and network seurity			
Course Code	CSE 324	Regular/ Elective	elective	
Contact Hours	Lectures	3	Tutorials	1
Course Assessment	Assessment Heading	Assessment Type	Contribution	
	Continuous Assessment	Assignments	10%	
		Tests	40%	
	Semester End Assessment	Examination	50%	
Course Outcomes	- Learn to identify security threats - Identify issues of privacy, authenticity, and security of information - Cryptographic techniques and their application to real-world network security			
Topics Covered	1	Computer Security Concepts, The OSI Security Architecture		
	2	Security Attacks, Security Services , Security Mechanisms, A Model for Network Security		
	3	Symmetric Cipher Model, Substitution Techniques		
	4	Transposition Techniques(T)		
	5	Block Cipher Principles		
	6	The Data Encryption Standard (DES)		
	7	A DES Example, The Strength of DES		
	8	The Origins AES, AES Structure(T)		

	9	AES Round Functions, AES Key Expansion	
	10	An AES Example	
	11	Example contd…	
	12	Multiple Encryption,Triple DES (T)	
	13	Block Cipher Modes of Operation -Electronic Codebook Mode, Cipher Block Chaining Mode	
	14	Cipher Feedback Mode	
	15	Output Feedback Mode, Counter Mode	
	16	Principles of Pseudorandom Number Generation, Pseudorandom Number Generators(T)	
	17	Pseudorandom Number Generation Using a Block Cipher	
	18	Stream Ciphers	
	19	RC4	
	20	Prime Numbers, Fermat’s and Euler’s theorems, Testing for primality(T)	
	21	Chinese Remainder Theorem	
	22	Public-Key Cryptography and RSA- Principles of Public-Key Cryptosystems	
	23	The RSA Algorithm	
	24	Diffie-Hellman Key Exchange(T)	
	25	Cryptographic Hash Functions -Applications	
	26	Two simple hash functions	
	27	Requirements and security	
	28	Hash Functions based on Cipher Block Chaining(T)	

	29	Secure Hash algorithm, SHA-3	
	30	Message Authentication Requirement, Message Authentication Function	
	31	Message Authentication codes	
	32	Digital Signatures(T)	
	33	Transport Level Security-Web Security Issues	
	34	Secure Sockets Layer (SSL)	
	35	Transport Layer Security	
	36	Electronic Mail Security(T)	
	37	Pretty Good Privacy	
	38	S/MIME	
	39	IP Security- IP Security Overview, IP Security Policy	
	40	Encapsulating Security Payload(T)	
	41	Combining Security Associations	
	42	Internet Key Exchange	
	43	Intruders, Intrusion Detection	
	44	Password management(T)	
	45	Malicious software –Types,Viruses	
	46	Viruses Countermeasures, worms	
	47	Need for Firewalls, Firewall Characteristics	
	48	Types of Firewalls(T)	

References	1. William Stallings - Cryptography and Network Security: Principles and Practice, Prentice Hall, 5th edition, 2010. 2. Behrouz A. Forouzan and Debdeep Mukhopadhyay - Cryptography and Network Security, Mc Graw Hill, 2nd Edition ,2008.