

The Maharaja Sayajirao University of Baroda Polytechnic Higher Payment Program Diploma in Computer Engineering			ACADEMIC YEAR 2021-2022	
Year	III	NETWORK SECURITY (CSE3617)	Lecture Hrs per week	4
Semester	II		Max marks	100
Pre-requisite: Basic Mathematical concepts: Random numbers, Number theory.				
CO1	Explain fundamental security concepts including security goals, OSI security architecture, attacks and authorization and authentication.			
CO2	Apply symmetric-key encryption techniques such as classical substitution/transposition methods, DES and block cipher design principles.			
CO3	Assess advanced encryption systems including AES structure, block cipher modes and random number generation for maintaining confidentiality.			
CO4	Explain and evaluate public-key cryptosystems like RSA, Diffie–Hellman. Assess message authentication codes and digital signatures for authentication.			
CO5	Assess network and system security mechanisms including Kerberos and study secure email protocols (PGP, S/MIME).			
BT	1. Remember 2. Understand 3. Application 4. Analysis 5. Evaluation 6. Creation			
COURSE CONTENT/SYLLABUS				
Unit	Unit Name	Hrs	Weightage	CO
Unit-1	Concept of Security: Security Trends, Security Goal, The OSI Security Architecture, Security Services, Mechanisms and Attacks, A Model for Network Security, Concepts of Authorization and Authentication.	8	12	CO1
Unit-2	Symmetric Ciphers: Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines, Steganography. Block Ciphers and Data Encryption: Block Ciphers Principles, Data Encryption Standard, The strength of DES, Block Cipher Design Principles.	12	22	CO2
Unit-3	Advanced Encryption Standard: Evaluation Criteria for AES, The AES Cipher, Block Cipher Modes of Operation. Confidentiality using symmetric encryption: Placement of encryption Function, Traffic Confidentiality, Key Distribution, Random Number Generation.	10	18	CO2, CO3
Unit-4	Public-Key Encryption: Principles of Public-key Cryptosystems, RSA, Key Management in public-key cryptosystem, Diffie-Hellman Key Exchange, Message Authentication: Authentication Requirements, Authentication Functions, Message Authentication Codes, Digital Signatures	10	18	CO4
Unit-5	Network Security Applications: Kerberos, X.509 Authentication Service, Public Key Infrastructure, Electronic Mail Security: Pretty Good Privacy, S/MIME	10	18	CO5
Unit-6	System security: Intruders, Intrusion Detection, Password Management, Viruses and related threats, Firewalls	8	12	CO5
		58	100	
REFERENCE BOOKS:				
1.	Network Security Essentials (2nd edition), William Stallings, Prentice Hall. 2003.			
2.	Network Security Principles and Practices (CCIE Professional Development). Saadat Malik, Saadat Malik. Pearson Education. 2002			
3.	Cryptography and Network Security, By Stallings William, William Stallings, Pearson Publication Inc.			
4.	Cryptography & Network Security By Forouzan			
5.	Cryptography and Network Security, Atul Kahate, Tata McGraw-Hill Education			
6.	Computer Security Basics, Deborah Russell, G. T. Gangemi, O'Reilly Media, Inc.			

7.	Computer Security, Dieter Gollmann, John Wiley & Sons
8.	Network Security: Private Communication in a Public World, By Kaufman Charlie and Perlman Radia
9.	Network Security: A Beginners Guide , by Eric Maiwald

