Walchand College of Engineering, Sangli
(Government Aided Autonomous Institute)

AY 2024-25

Course Information

Programme	B.Tech. (Information Technology)
Class, Semester	Final Year B. Tech., Sem. VII
Course Code	
Course Name	Cryptography & Network Security
Desired Requisites:	Computer Networks

Teaching Scheme		**Examination Scheme (Marks)**			
Lecture	3 Hrs/week	**MSE**	**ISE**	**ESE**	**Total**
Tutorial	-	30	20	50	100
	-	**Credits: 3**			

Course Objectives

1	To describe the fundamental concepts of network security using confidentiality, integrity and availability (CIA) of the information
2	To explain various encryption techniques
3	To apprise security mechanisms and services against threats

Course Outcomes (CO) with Bloom's Taxonomy Level

At the end of the course, the students will be able to,

CO	**Course Outcome Statement/s**	**Bloom's Taxonomy Level**	**Bloom's Taxonomy Description**
CO1	Extend number coding theory in view of information security aspects	II	Understanding
CO2	Practice various crypt-complex encryption algorithms providing confidentiality	III	Applying
CO3	Compare access control mechanisms and authentication services resolving the security issues	IV	Analyzing
CO4	Recommend mathematical functions that are able to check information integrity	V	Evaluating
CO5	Propose application of security framework at the desired network layer	VI	Creating

Module	**Module Contents**	**Hours**
I	**Security Overview:** Services, Mechanism and Attacks, The OSI Security Architecture, Classical Encryption Techniques, Substitution Techniques, Transposition Techniques, Steganography	7
II	**Block Cipher:** Block Cipher Design Principles, Modes of Data Transfer, Symmetric Cipher Model, Data Encryption Standard, Security of 2DES, 3DES & AES	7
III	**Public Key Encryption:** Principles of Public-Key Cryptosystem, RSA Algorithm, Distribution of Public Keys, Diffie-Hellman Key Exchange	6
IV	**Authentication Functions and Services:** Hash Functions, Message Authentication Codes, Digital Signatures Kerberos, X.509 Certificates	6
	IP & Web Security: IP Security Architecture, Authentication Header, Encapsulating Security	

V	Payload, Combining Security Associations Web Security Considerations, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction	6
VI	**Perimeter Security:** Intruders, Intruder Detection, Password Management, Malwares Firewall Configurations, Trusted Systems, Honeypots	7

Text Books	
1	William Stallings, *"Cryptography and Network Security, Principles and Practices",* Pearson Publication, 8th Edition 2020
2	Atul Kahate, *"Cryptography and Network Security",* McGraw Hill Education India, 4th Edition, 2017

References	
1	Menezes, A. J., P. C. Van Oarschot, and S. A. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 2nd Edition, 2018
2	Schneier, Bruce, "*Applied Cryptography: Protocols & Algorithms*", Wiley Publication,2nd Edition, 2015

Useful Links	
1	https://www.researchgate.net/publication/26585503_Network_Security_Policies_and_Guidelines_for_Effective_Network_Management
2	https://www.tutorialspoint.com/information_security_cyber_law/network_security.htm
3	https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008

CO-PO Mapping

	Programme Outcomes (PO)												**PSO**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	2										1		
CO2			1		3								2	
CO3		3				2	1							
CO4	2		3											1
CO5				2				1						3

The strength of mapping is to be written as 1: Low, 2: Medium, 3: High
Each CO of the course must map to at least one PO.

Assessment

The assessment is based on MSE, ISE and ESE.
MSE shall be typically on modules 1 to 3.
ISE shall be taken throughout the semester in the form of teacher's assessment. Mode of assessment can be field visit, assignments etc. and is expected to map at least one higher order PO.
ESE shall be on all modules with around 40% weightage on modules 1 to 3 and 60% weightage on modules 4 to 6.
For passing a theory course, Min. 40% marks in (MSE+ISE+ESE) are needed and Min. 40% marks in ESE are needed. (ESE shall be a separate head of passing)