Marwadi University

FACULTY OF COMPUTER APPLICATIONS

Bachelor of Science in information technology

Sem. : 5

Subject Code : 05BS0503

Subject : Cryptography

Objectives :

1. To understand the fundamentals of Cryptography
2. To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
3. To understand the various key distribution and management schemes.
4. To understand how to deploy encryption techniques to secure data in transit across data networks
5. To design security applications in the field of Information technology

Prerequisites : Mathematical concepts: Random numbers, Number theory, finite fields.

Unit No	Topics Covered	No of lectures required
1	**Introduction** Definition of computer security, CIA triad, Security attacks: Active & Passive attacks, Introduction of cryptography, Understand basic Encryption Concepts, Symmetric/Asymmetric Cipher Model, Introduction of Cryptanalysis and Brute force Attacks, Classification cryptography	08
2	**Classical Encryption algorithm:** Introduction of classical encryption, types of classical cryptography: Transposition cipher & substitution cipher, Substitution cipher : Ceaser cipher, playfair	12

	cipher. Transposition cipher: Rail fence cipher, row transposition cipher.	
3	**Modern Cryptography** Stream ciphers and block ciphers, Block Cipher structure, Feistel Cipher, Diffusion and Confusion, Data Encryption standard (DES).	**12**
4	**Public Key Cryptography:** Encryption & decryption with public key cryptography ,Basic terms of public key cryptography,RSA algorithm with example,Deffie Helman Key Exchange algorithm. Virus,Virus classification.	**8**
5	**Security authentication:** Introduction of biometric, characteristic, Boi-metric process, finger print recognition, Iris identification, Vein recognition ,signature verification process, Application of biometric, Advantage & disadvantage of biometric.	**12**

Course Outcomes

1. Understanding the concepts of cryptography security and their use.
2. Understanding of principles & algorithms of classical cryptography.
3. Understand and use of modern cryptography algorithm.
4. Understand the concepts of public key cryptography & types of threats
5. Understand of biometric authentication & its techniques.

Course Outcomes – Program Outcomes Mapping Table :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	M					H		L
CO2			L			M		
CO3	L					H		M
CO4		H				L		M

CO5	M		H					L

Text Book :

1. "Cryptography and Network Security – Principles and Practice", William Stallings : 5/E, Pearson Education.
2. "Introduction to biometrics", Anil k Jain , Dr.Arun k ross, Dr.Karthik nanadakumar, Springer-Latest edition 2011.

Reference Books :

1. Bruce Scheneir : "Applied Cryptography", 2/E, John Wiley,1996
2. Behrouz Forouzan : "Cryptography & Network Security", 1/E,TMH,2007
3. Menezes, Oorschot, Vanstone : "Handbook of Applied Cryptography", CRC Press,1996
4. D Stinson, "Cryptography: Theory and Practice", 2/E,Chapman & Hall ,2002

Web References:

1. https://www.ijsr.net/conf/NCKITE2015/100.pdf
2. https://www.tutorialspoint.com/cryptography/
3. https://freevideolectures.com/course/3027/cryptography-and-network-security
4. https://nptel.ac.in/courses/106105031/
5. https://www.mepits.com/tutorial/413/basic-electronics/smart-cards

App Reference :

1. Cryptography - Collection of ciphers and hashes

Syllabus Coverage from Main reference:

Unit #	Chapter Numbers
1	Book-1: Chapter 1: 1.1,1.3 Chapter 2: 2.1
2	Book-1: Chapter 2 : 2.2 ,2.3
3	Book-1: Chapter 3: 3.1,3.2
4	Book-1 : Chapter 9: 9.1,9.2, Chapter 10: 10.1 , Chapter 21: 21.2
5	Book-2 : Chapter 2: 2.1, Chapter 3: 3.1, Chapter 4: 4.1 & Web ref-1

Marwadi University

FACULTY OF COMPUTER APPLICATIONS

Bachelor of Science in information technology

PRACTICALS

Sr.No	List of Practical
1	Program related to concepts of Python (loop, range, lambda function, data structures)
2	Basic programs exercise & introduction of packages for cryptography
3	Implementation of encryption of message using ceaser cipher.
4	Implementation of Decryption of message using ceaser cipher algorithm.
5	Implementation of hacking of ceaser cipher algorithm.
6	Implementation of encryption and decryption of message using FERNET cryptography package.
7	Implementation of RSA algorithm in python.
8	Implementation of DES in python
9	Implementation of AES
10	Implementation of MD5

Note : Use Python 3.0 for implementation of algorithms.