FACULTY OF COMPUTER APPLICATIONS
Bachelor Of Computer Applications (Hons.)

- **Sem.** : 7
- **Subject Code** : 05BH0703
- **Subject** : Cryptography
- **Course Objectives** :

1. **Develop a holistic understanding of information security:** Students will gain a broad and interconnected view of the principles, techniques, and challenges in securing computer systems and information.
2. **Cultivate critical thinking skills in analyzing security vulnerabilities and solutions:** Students will learn to assess security threats, evaluate the effectiveness of different security measures, and make informed decisions regarding security implementations.
3. **Gain practical awareness of cryptographic tools and their applications in real-world scenarios:** Students will understand how cryptographic techniques are employed to achieve confidentiality, integrity, and authentication in various applications and systems.
4. **Foster an appreciation for the evolving landscape of cyber security threats and defenses:** Students will develop an understanding of the dynamic nature of security challenges and the ongoing need for adaptation and innovation in security practices.
5. **Establish a foundational knowledge base for further specialized study in cyber security:** This course will provide students with the essential concepts and terminology necessary to pursue more advanced topics in specific areas of computer security and cryptography.

FACULTY OF COMPUTER APPLICATIONS
Bachelor Of Computer Applications (Hons.)

- **Prerequisites**: Basic Computer networking and number system.

Unit No	Topics Covered	No of lectures required
1	**Introduction** 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, Substitution techniques: Ceasar cipher, Play fair cipher, Transposition techniques : Rail fence Cipher and Row transposition cipher	08
2	**Symmetric key Cryptography** Stream ciphers and block ciphers, Block Cipher structure, Feistel Cipher, Diffusion and Confusion, Data Encryption standard (DES), strength of DES, Design principles of block cipher, Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	10
3	**Public Key Cryptography & Authentication application** **Public Key Cryptography** Encryption & decryption with public key cryptography, Basic terms of public key cryptography, RSA algorithm with example, Diffie Helman Key Exchange Algorithm **Authentication application** Digital Signatures, Kerberos, X.509.	10
4	**Hashing Techniques** Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining. Secure Hash Algorithm (SHA).	05
5	**System Security** Intruders, Intrusion Detection, Virus and Worms, Virus Counter-Measures, DDOS attack, Firewall. **Other Security Issues** Smart Cards and Security, Zero Knowledge Protocol, Biometric Authentication: characteristic, Bio-metric process, finger print recognition, Iris identification, Vein recognition, signature verification process,	12

	Application of biometric, Advantage & disadvantage of biometric.	

Course Outcomes:

1. Upon completing this course, students will be able to synthesize knowledge from various security domains to explain the holistic approach to securing computer systems and information.
2. Students will be able to analyze potential vulnerabilities in systems and networks and justify the selection and implementation of appropriate security solutions based on their effectiveness and limitations.
3. Students will be able to identify scenarios where different cryptographic methods are used and articulate how they contribute to confidentiality, integrity, and authentication in those contexts.
4. Students will be able to describe how threats and defenses evolve over time and understand the need for ongoing professional development in the field of cyber security.
5. Students will be well-prepared to pursue further specialized learning in specific areas of cyber security, building upon the knowledge gained in this course.

Course Outcomes – Program Outcomes Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	H	M	L	L	L	L	M	L
CO2	M	H	M	L	L	M	M	M
CO3	H	M	M	L	L	M	M	M
CO4	L	M	L	M	L	H	H	M
CO5	M	M	L	L	L	L	H	L

Text Book :

1. "Cryptography and Network Security – Principles and Practice", William Stallings, Pearson Education, 5th Edition.

Reference Books :

1. "Applied Cryptography", Bruce Scheneir, John Wiley, 2nd Edition.
2. "Cryptography and Network Security", Behrouz Forouzan, TMH, 1st Edition.

3. "Handbook of Applied Cryptography", Menezes, Oorschot, Vanstone CRC Press.

Web References:

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

App References:

1. Cryptography - Collection of ciphers and hashes
2. Decrypto

Syllabus Coverage from text /reference book & web/app reference:

Unit #	Chapter Numbers
1	Chapter 1: 1.1 to 1.6 and Chapter 2: 2.2 and 2.3
2	Chapter 2:2.1 Chapter 3: 3.1 to 3.5, Chapter 5:5.1 to 5.5 Chapter 6: 6.1 to 6.6, Chapter 7: 7.4 and 7.5, Chapter 9: 9.1, 9.2 and Chapter 10: 10.1
3	Chapter 13: 13.1, Chapter 15: 15.3
4	Chapter 11: 11.1 to 11.6
5	Chapter 16: 16.1,16.2, 16.3, Chapter 18: 18.1,18.2, Chapter 17: 17.1 to 17.3, Chapter 20,21 and 22

Marwadi University
Marwadi Chandarana Group

NAAC A+

FACULTY OF COMPUTER APPLICATIONS
Bachelor Of Computer Applications (Hons.)

PRACTICALS

Note: Programming language for lab is Python

Sr. No	List of Practical
1	Write a program that contains a string with a value "Hello World'. The program should XOR each character in this string with 0 and displays the result.
2	Basic programs exercise & introduction of packages for cryptography.
3	Write program to implement Caesar cipher.
4	Write a program to implement 2x2 Hill cipher.
5	Write a program to implement Rail fence cipher.
6	Write a program to implement encryption and decryption of message using FERNET cryptography package.
7	Write a program to implement RSA algorithm in python.
8	Write a program to implement DES in python.
9	Write a program to implement encryption and decryption using DES algorithm in ECB, CBC and CFM mode. Take plain text and key from user.
10	Write a program for implementing Diffie Hellman key exchange algorithm.
11	Write a program to implement MD5.
12	Create a Manu driven program for implementing DES, AES, RC4, RSA, Diffie Hellman, MD5 and SHA algorithm.