Marwadi University
Faculty of Diploma Studies
Information and Communication Technology

Subject Code: 09CT0503

Subject Name: Cryptography and Network Security

Semester -V

Objective: Cryptography is an indispensable tool for protecting information in computer systems. It deals with the algorithmic and mathematical perspective of information and network security. In this course you will learn the inner workings of cryptographic systems and how to correctly use them in real-world applications.

Credits Earned: 05 Credits

Course Outcomes:

After the completion of the course, the students will be able to:

- Compare Various Cryptanalysis Techniques. (Understand)
- Apply the knowledge in the applications ranging from small scale to larger scale security systems. (Apply)
- Apply knowledge in interpreting the secured systems for real world problems. (Apply)
- Analyse the encryption standards and the security strengths of the applied cryptographic algorithm (Analyse)
- Evaluate the performance of the given case study application and solve the fault to improve the security standards (Evaluate)

Pre-requisite of course: Computer Networks, Discrete Probability

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Term work (TW)	
4	0	2	5	50	30	20	25	25	150

Contents:

Unit	Topics	Contact Hours
1	**Security in Computing Environment:** Need for Security; Security Attack – Threats, Vulnerabilities, and Controls, Types of Threats (Attacks); Security Services – Confidentiality, Integrity, Availability; Information Security; Methods of Protection.	4

2	**Basics of Cryptography:** Terminologies used in Cryptography; Substitution Techniques – The Caesar Cipher, One-Time Pads, The Vernam Cipher, Book Cipher; Transposition Techniques – Encipherment/Decipherment Complexity, Digrams, Trigrams, and Other Patterns, pseudo Random Generators	8
3	**Symmetric Key Encryption:** Block Ciphers, Cipher Block Chaining Mode, Data Encryption Standard (DES) Algorithm – Overview of the DES Algorithm; Double and Triple DES – Double DES, Triple DES; Security of the DES; Advanced Encryption Standard (AES) Algorithm, AES Expansion, PRG using Block Cipher	12
4	**Public Key Encryption:** Integer Factorization Problems, Characteristics of Public Key System; RSA Technique – Encryption-Method; Key Exchange; Diffie-Hellman Scheme; ElGamal, Elliptic Curve Cryptography, Security analysis	10
5	**MESSAGE AUTHENTICATION AND INTEGRITY** **A**uthentication requirement, Authentication function, CBC-MAC, SHA, MD5, HMAC, Birthday Attack, Hash function, Security of hash function, Digital signature, Biometrics, Passwords, authentication protocols, Kerberos	9
6	**Network Security:** Network Concepts; Threats in Networks – Who Attacks Networks? Threats in Transit: Eavesdropping and Wiretapping, Protocol Flaws, Impersonation; DOS, DDOS, Man in the Middle Attacks, Network Security Controls – Architecture, Encryption, Virtual Private Networks, Public Key Infrastructure (PKI) and Certificates.	8
	Total	**51 hrs**

References:

1. Cryptography and Network Security Principles and Practices, 6th edition – Atul Kahate [Tata-McGraw-Hill]
2. Cryptography and Network Security Principles and Practices, 5th edition -- William Stallings [Prentice Hall]
3. Introduction to Cryptography with Coding Theory -- Washington & Trappe [Pearson].
4. Applied Cryptography: Protocols, Algorithms, and Source Code in C -- Bruce Schneier, [John Wiley & Sons].

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

R Level	U Level	A Level	N Level	E Level	C Level
10	**30**	**10**	**10**	**5**	**5**

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Suggested List of Practical:

1. Implement Shift Cipher
2. Implement One Time Pad Cipher
3. Implement Playfair Cipher
4. Implement Hill Cipher
5. Implement Vigenere Cipher
6. Implement Rail Fence Cipher
7. Implement RSA cipher
8. Understand DES cipher implementation
9. Understand AES cipher implementation
10. Understand MAC implementation

Instructional Method:

a. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

b. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

c. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory

Supplementary Resources:

1. https://www.coursera.org/learn/crypto
2. https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/
3. https://www.udacity.com/course/applied-cryptography--cs387
4. https://www.classcentral.com/course/crypto-616
5. https://www.edx.org/learn/cryptography