Marwadi University
Faculty of Diploma studies
Information and Communication Technology

Subject Code: 09CT0610

Subject Name: Cyber Security

Diploma Year – III (Semester VI)

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: 04 Credits

Course Outcomes:

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

1. To categorize common types of security threats are risks to the Computer Systems and the nature of common Information hazards.
2. Identify the potential threats to confidentiality, integrity and availability of Computer Systems at personal and organizational level.
3. Gain understanding of different requirements and principles for Electronic Mail, IP Security and Web Security with monitoring and analysis of networks.
4. Gain the understanding and requirements of different firewalls and other wireless security standards.

Pre-requisite of course: Computer Networks, Discrete Probability, Cryptography

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)	
3	0	2	4	50	30	20	25	25	150

Contents:

Unit	Topics	Contact Hours
1	**Introduction and Security Threats:** Threats to security: Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare Avenues of Attack, steps in attack, Security Basics –Confidentiality, Integrity, Availability Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection. Malware: Viruses, Logic bombs	**5**
2	**Organizational Security** Password selection, Piggybacking, Shoulder surfing, Dumpster diving, Installing unauthorized software, hardware, Access by non-employees. People as Security Tool: Security awareness,and Individual user responsibilities. Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers	6
3	**IP Security:** Overview of IP Security (IPSec); IP Security Architecture; Modes of Operation; Security Associations (SA) – Security Parameter Index (SPI), SA Management, Security Policy; Authentication Header (AH); Internet Key Exchange	8
4	**Web Security:** Web Security Requirements; Secure Socket Layer (SSL) – SSL Architecture, SSL Protocol; Transport Layer Security (TLS); Secure Electronic Transaction (SET) – Features, Components, Dual Signature, Purchase Request.	9
5	**Electronic Mail Security:** Threats to E-Mail; Requirements and Solutions – Confidentiality, Integrity; Encryption for Secure E-Mail; Secure E-Mail System – PGP (Pretty Good Privacy), S/MIME (Secure Multipurpose Internet Mail Extensions).	8
6	**Firewalls:** Firewalls, Types, Packet Filtering Gateway, Stateful Inspection Firewall, Application Proxy, Guard, Personal Firewalls	4
7	**Wireless Network Security Standards** IEEE 802.11, IEEE 802.11i Wireless LAN Security, WAP protocol, WAP End-to-End Security	**3**
	Total	**43 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. Cryptography and Network Security – B A Forouzen [TMH]
4. Computer Security – Dieter Gollman [Wiley India Education, Second Edition]
5. Computer Security Basics – Deborah Russell G.T. Gangenisr [O'Reilly Publication]

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)

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyse	Evaluate	Create
10%	10%	40%	20%	10%	10%

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