MCA 308 Cryptography and Cyber Security

Teaching Scheme	**Examination Scheme**
Lectures: 3 hrs/Week	Class Test -12Marks
Tutorials: 1 hr/Week	Teachers Assessment - 6Marks
	Attendance – 12 Marks
Credits: 4	End Semester Exam – 70 marks

Prerequisite: - MCA 101 Computer Concepts and C programming, MCA 303 Data Communication & Computer Network

Course Objectives:

1- To define cryptography, its use, areas where cryptography is needed.

2- To understand security concepts, ethics in Network Security, security threats, and the security services and mathematical foundation required for various cryptographic algorithms.

3- To develop code to implement a cryptographic algorithm or write an analysis report on any existing security product.

4- To analyze all key less and keyed algorithms to identify their strength and weaknesses and try to solve and remove the limitations or optimize the complexity of algorithm(s).

5- To test different available algorithms in terms of complexity, response time, key size, data size, security assurance, etc.

6- To design an algorithmic solution of a problem either by applying existing algorithms or a new one. Identify and classify computer and security threats and develop a security model to prevent, detect and recover from attacks.

Detailed Syllabus

UNIT I

Introduction to Cryptography and Network Security: Security Goals, Attacks, Services and Mechanisms, Techniques, Traditional Symmetric Key Cipher.

UNIT II

Modern Symmetric Key Ciphers: Fiestal Cipher, S-DES, DES, Double DES, Triple DES, AES, Block Cipher. Modes of Operation : ECB, CBC, CFB, OFB and CTR, KDC.

UNIT III (10 Hours)

Introduction to Mathematics for Cryptography: Modular Arithmetic, The Euclidian Algorithm, Extended Euclid, Farmet's and Euler's Theorem, Chinese Remainder Theorem.

UNIT IV (10 Hours)

Asymmetric Key Cryptography: RSA Algorithm, ECC, Key Management- Public Key Distribution, Sharing of secret key using A-symmetric Key Cryptosystem.

UNIT V (10 Hours)

Message Authentication: MAC, SHA-512 and MD5. Digital Signature: DSS Key Management: Symmetric Key Distribution, Kerberos.

UNIT VI (10 Hours)

Network Security: IPSec, SSL and TSL, PGP AND S/MIME, SET, System Security: Malicious Software, Firewalls and Intruders.

Head
Department of Computer Applications
Faculty of Computer Applications
Invertis University, Bareilly (U.P.)

Registrar
Invertis University
Bareilly

Dean Academics
Faculty of Computer Applications
Invertis University, Bareilly (UP)

Text and Reference Books

1. Cryptography and Network Security, Behrouz A Frouzan, TMH, 1st Edition 2007.
2. Cryptography and Network Security, William Stalling, Pearson Education, 4th Edition, 2006.
3. Applied Cryptography, Bruce Schinner, Willy and Sons, 2nd Edition 1996.

Course Outcomes:

After completing the course, students will be able to:

1. Identify some of the factors driving the need for network security.
2. Identify and classify particular examples of attacks.
3. Define the terms vulnerability, threat and attack.
4. Identify physical points of vulnerability in simple networks.
5. Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.