CSH407: Cryptography and Data Security	
Teaching Scheme Lectures: 4 hrs/Week Tutorials: 2 hr/Week Credits: 6	**Examination Scheme** Class Test -20 Marks Teachers Assessment – 10 Marks Attendance – 20 Marks End Semester Exam – 100 marks

Prerequisite: - BCA 203 C Programming, BCA 304 Computer Networking.

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.
3- To develop code to implement a cryptographic algorithm using any programming language.
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-1 **Introduction to Cryptography:** Introduction To Security Attacks, Services & Mechanisms, And Conventional Encryption: Classical Techniques, cryptanalytic attacks.
Unit-2 **Private Key Encryption:** Modern Techniques: Simplified DES, Block Cipher Principles, DES Standard, Double DES, Triples DES.
Unit-3 **Public Key Encryption:** Public-Key Cryptography: Principles of Public-Key Cryptosystems, RSA Algorithm, public key distribution, symmetric key distribution using asymmetric cryptosystem.
Unit-4 **Hash Functions:** Message Authentication & Hash Functions, Authentication Functions, Message Authentication Codes (MAC), Secure Hash Algorithm (SHA), Digital Signatures.
Unit-5 **Application Layer Security:** Electronic Mail Security, Pretty Good Privacy (PGP).**Transport Layer Security:** Secure Socket Layer & Transport Layer Security. **Network Layer Security:** Authentication Header, Encapsulating Security Payloads.
Unit – 6 **Network and System Security:** Authentication Applications-Kerberos X.509, Secure Electronic Transaction (Set), System Security: Intruders, Viruses, Firewall Design Principles.

Text and Reference Books

1. Cryptography and Network Security: Principles and Practice, William Stallings, Prentice Hall, New Jersey, 4th Edition.
2. Introduction to cryptography, Johannes A. Buchmann, Springer, Verlag, 2001.
3. Cryptography and Network Security, Atul Kahate, TMH, 2nd Edition.
4. Cryptography, Forouzan, TMH, 2007.

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.