# Cryptography

1.1 Course Number: CS430

1.2 Contact Hours 3-0-2 Credits: 11

1.3 Semester-offered: 7

1.4 Prerequisite: Computer Network

1.5 Syllabus Committee Member:

2. **Objective:** The objective of the course is to present an introduction to Cryptography, with an emphasis on how to protect the information security from unauthorized users.

3. **Course Content:**

Unit-wise distribution of content and number of lectures

| **Unit** | **Topics** | **Sub-topic** | **Lectures** |
|---|---|---|---|
| 1 | Introduction | Threats, vulnerabilities and attacks. Authentication, confidentiality, integrity and non-repudiation in data communication, Mathematical Tools for Cryptography, Classical Cryptosystems | 8 |
| 2 | Private key cryptosystems | Stream and Block cipher, Feistel Cipher, DES, AES, RC4, Mode of operations | 9 |
| 3 | Public key cryptosystems | Knapsack cryptosystems, RSA; Attacks on RSA, Diffie Hellman Key Exchange, Discrete Logarithm problem, ElGamal cryptosystems, Elliptic Curve cryptosystems | 10 |
| 4 | Cryptographic Hash function and authentication | Properties and applications of the cryptographic hash. SHA-1, MD5, MD5, SHA-512, Message authentication Code (MAC) and the digital signature. | 9 |
| 5 | Key management | Key management, digital certificates and the Public Key Infrastructure (PKI) | 5 |
| | | **Total** | **41** |

## 4. Readings

4.1 Textbook: Cryptography and Network Security B.Forouzan. Tata McGraw Hill.
4.2 Reference books:

1. Cryptography and Network Security - Principles and Practices, W. Stallings, Pearson Education Publishers
2. Several papers from conferences, magazines and journals

## 5 Outcome of the Course:

- Have a broad understanding of Cryptography course.
- Have a high-level understanding of cryptographic based different applications and their functionality.
- Be able to model secure applications based on the knowledge of cryptography.