राष्ट्रीय प्रौद्योगिकी संस्थान जमशेदपुर
NATIONAL INSTITUTE OF TECHNOLOGY JAMSHEDPUR
(An Institution of National Importance under MHRD, Government of India)

Department of Computer Applications

Autumn Semester 2020-21

Course File

Course Code	: CA4102
Course Title	: Cryptographic Foundation
Batch	: M. Tech (ISSE) I Semester
Faculty In-charge	: Dr. Alekha Kumar Mishra
E-mail	: alekha.ca@nitjsr.ac.in
Contact number	: 8249803116

Course Description: This course provides an introduction to classical and modern cryptography techniques. It focuses on the backgraound mathematics related to cryptography and how cryptographic algorithms works and implemented. The elements covered in this course are basics of number theory, symmetric encryptions, assymetric encryptions, message authetication codes, and digital signatures. Basic cryptanalytic techniques and examples of practical security solutions are explored to understand how to design and evaluate modern security solutions.

Course Objectives:

i) Built the mathematical foundation to learn cryptography.
ii) Learn various types of classical and morden cryptographic techniques that includes symmetric encryptions, assymetric encryptions, cryptographic hashing and digital signatures.
iii) Analyze the strength and weakness of each cryptographic techniques
iv) To implement and apply the cryptographic techniques.

Course Outcomes:

i) Students will get to know basic principles of cryptography and general cryptanalysis
ii) Be acquainted with the concepts of symmetric encryption and authentication as well as public key encryption, digital signatures and cryptographic hashing techniques.
iii) Implement and execute cryptographic mechanisms and compare their performance.
iv) Be able to compose, build and analyze simple cryptographic solutions.

Text / Reference Books:

1) “Cryptography and Network Security: Principles and Practice” by William Stallings, 7th Edition, Pearson

2) “Cryptography and Network Security” by Behrouz A Forouzan and Debdeep Mukhopadhyay, McGraw Hill
3) “Cryptography and Network Security” by Atul Kahate

Course Plan:

Lecture – 1	Introduction to Cryptography; Security Attacks – Security Services – Security Mechanisms
Lecture – 2	Classical Cryptography; Symmetric Cipher Model
Lecture – 3	Basic Concepts of Modular Arithmetic; GCD algorithm; Extended GCD Algorithm
Lecture – 4	Substitution Techniques
Lecture – 5	Substitution Techniques contd..
Lecture – 6	Transposition Techniques; Concepts of Block Cipher
Lectures – 7-8	DES Algorithm
Lecture –9	DES Example
Lectures – 10-12	AES Algorithm
Lectures – 13-14	AES Example
Lecture – 15	Multiple Encryption
Lecture – 16	Triple DES with example
Lecture – 17	Cipher Block Chaining
Lecture – 18	Concept of Prime Number
Lecture – 19	Principles of Pseudo Random Number Generation
Lecture – 20	Stream Ciphers; RC4
Lecture – 21	Discrete Cosine Transform
Lecture – 22	Fermat’s Theorem; Euler’s Theorem; Test for primality
Lecture – 23	Public Key Cryptosystems
Lecture – 24-25	RSA algorithm with example
Lecture – 26	Diffie-Hellman Key Exchange
Lecture – 27	El Gamal Cryptosystem
Lecture – 28-29	ECC
Lecture – 30	Cryptographic Hash Functions
Lecture – 31	SHA 512
Lecture – 32	Overview of Message Authentic Codes
Lecture – 33-34	Digital Signatures
Lecture – 35	Summary

Evaluation Scheme:

S.No.	Evaluation Component	Weightage	Nature of Component
1	Mid-term Examination	30%	Online Mode
2	End-term Examination	40%	Online Mode
3	Teacher’s Assessment	30%	Paper presentation, Technical report, Attendance

Consultation Hours: Mon, Tue, Thu, Fri - 3 to 4 PM.

Dr. Alekha Kumar Mishra.