BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, Pilani

SECOND SEMESTER 2020-2021

Course Handout (Part-II)

Date: 16-01-2021

In addition to Part I (General Handout for all courses appended to the time table) this portion gives further specific details regarding the course.

Course No. : **MATH F441**
Course Title : **Discrete Mathematical Structures**
Instructor-in-charge : **S. Dey**

1. Scope and Objective of the course:

The objective is to present and discuss some of the methods of discrete mathematics and some discrete mathematical structures at graduate level. The first part deals with some functions and techniques of discrete nature used in design and analysis of algorithms and the second part deals with Combinatorial Structures and algorithm. (Since there is a separate course offered on Graph theory, graphical structures are not discussed in detail in this course)

2. Text Books:

1) *Lindsay Childs*, A Concrete Introduction to Higher Algebra-2e, Springer-Verlag, 1979.

2) *V. Krishnamurthy***,** Combinatorics, Theory and Applications, East-West Press, 1985.

Reference Books:

(1) C. Carlet. **Boolean function for Cryptography and Error Correcting Codes. Cambridge University Press (2007).**

(2) *R. Lide and H. Niederreiter*, **Introduction to finite fields & their applications, Cambridge University Press, 1986.**

(3) *Douglas R. Stinson, Maura B. Paterson.* **Cryptography, Theory and Practice. Fourth Edition.**

3. Course Plan:

Lect No.	Learning Objectives	Topic	Chapters	Book
1-4	Introduction to Groups	Definition and examples of groups. $\mathbf{Z}_n$ and Permutation group S_n,	9-E, 11-A,B 8-A,B 2 (Part-IV)	T-1 T-1 T-2
5-10	Introduction to the number theory and its application	Order of Element, Fermat's Theorem, Euler's φ function, Euler's theorem, RSA Codes	9-A 9-B 9-C 10-B	T-1 T-1 T-1 T-1

11-15	The Chinese remainder theorem (CRT)	CRT for integers CRT for polynomials Application of CRT to fast polynomial multiplication	12-A,C 20 21-B	T-1
16-24	Introduction to the theory of finite fields and Boolean Function	Construction of finite fields and simple field extension, Representation of Boolean function, Discrete Fourier Transformation, Fast Fourier Transformation	28-A,B 30-C, 2.1, 2.2	T-1 T-1 R-1 R-1
25-32	Introduction to several Algorithms	Algorithm for Differential Cryptanalysis, Linear Cryptanalysis, Correlation and Algebraic Attack	4.3, 4.4, 4.8.1, 4.8.2	R-3
33-35	Factoring in Q[x]	Eisenstein's criteria for Irreducibility	18	T-1
36-40	Introduction to Design	Latin square and Hadamard matrix	29-A Part-VIII	T-1 T-2

4. Evaluation Scheme:

EC No.	Evaluation Component	Weightage (Out of 100)	Date & Time	Nature of Component
1.	Quiz 1	15	To be announced	Open Book
2.	Mid-Semester	30	To be announced	Open Book
3.	Assignment	5	To be announced	Open Book
3.	Quiz 2	15	To be announced	Open Book
4	Comprehensive Examination	35	To be announced	Open Book

5. Make-up: Make-up will be given only in genuine cases.

6. Chamber consultation hour: To be announced in the class.

7. Notices: All notices regarding MATH F441 will be put up on CMS website only.

Instructor-In-Charge
MATH F441