University of Kerala

Discipline	Mathematics				
Course Code	UK2MDCMAT103				
Course Title	Introduction to Modular Arithmetic and Cryptography				
Type of Course	MDC				
Semester	II				
Academic Level	100-199				
Course Details	Credit	Lecture per week	Tutorial per week	Practical per week	Total Hours per week
	3	3			3
Pre-requisites	Basic properties of integers, divisibility, gcd Linear Diophantine equations, Unique factorization				
Course Summary	This is a short introduction to Cryptography using congruences.				

Detailed Syllabus

Module	Unit	Contents	Hrs
I		**Modular Arithmetic**	**9**
	1	Definition of congruence relation, Modular exponentiation, Divisibility tests, linear congruences, (Chapter 5: Sections 5.1, 5.2, 5.3, 5.4 of Text[1])	
II		**Three Classical Theorems**	**9**
	2	The Chinese remainder theorem, Fermat's theorem, Euler's theorem (Chapter 5: Sections 5.5, Chapter 6: Section 6.1, 6.2 of Text[1])	
III		**Introduction to Cryptography**	**9**
	3	Shift and affine cipher, Vigenere ciphers, transposition ciphers (Chapter 7: Sections 7.1, 7.2, 7.3, 7.4 of Text[1])	

Module	Unit	Contents	Hrs
IV	**RSA and applications**		**9**
	4	RSA, stream ciphers (Chapter 7: Sections 7.5, 7.6 of Text[1])	
V	**Suggestions for the teacher designed module**		**9**
	For internal assessment examinations only.		
	5	Wilson's theorem, Block ciphers, Secret sharing	
	These topics can be found on Chapters 6 and 7 of Text [1]		

Textbook

1. James S.Kraft, Lawrence C. Washington. Elementary Number Theory, CRC Press, 2015.

References

1. James S.Kraft, Lawrence C. Washington, An Introduction to Number Theory with Cryptography, CRC Press, 2014.
2. G A Jones, J M Jones, Elementary Number Theory, Springer, 1998.
3. Thomas Koshy, Elementary Number Theory with Applications, 2^{nd} Edition, Academic Press, 2007.

Course Outcomes

CO No.	Upon completion of the course the graduate will be able to	PO/PSO	Cognitive Level	Knowledge Category	Lecture(L) Tutorial (T)	Assignment (As)
CO 1	Describe the basic concept of Modular arithmetic	PSO1, PSO2	R	F,C	L	
CO 2	Apply congruence to solve various problems.	PSO3	U,Ap	P	L	
CO 3	Analyse the properties of integers using congruences via three milestone theorems	PSO3, PSO4	U,An	C	L	
CO 4	Apply congruence to cryptography	PSO3	R,U,An	C	L	

(R-Remember, U-Understand, Ap-Apply, An-Analyse, E-Evaluate, C-Create)
(F-Factual, C-Conceptual, P-Procedural, M-Metacognitive)

Mapping of CO with PSOs and POs

	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8
CO1	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO2	-	-	3	-	-	-	-	-	-	-	-	-	-	-
CO3	-	-	1	2	-	-	-	-	-	-	-	-	-	-
CO4	-	-	3	-	-	-	-	-	-	-	-	-	-	-

(- -Nill, 1-Slightly/Low, 2-Moderate/Medium, 3-Substantial/High)

Assessment Rubrics

- Quiz/Assignment/Discussion/Seminar
- Midterm Exam
- Programming Assignments
- Final Exam

Mapping of COs to Assessment Rubrics

	Internal Examination	Assignment	Project Evaluation	End Semester Exam
CO1	✓			✓
CO2	✓	✓		✓
CO3	✓			✓
CO4		✓		✓