Syllabus template

Semester: 8	
Programme: Mathematics	
Course: Algebra-6 and Mathematical Cryptography	
Paper code: C4MT230811T	
Hours/Week: 4	**Credits: 6**
Category: Core/MDC/SEC/VAC: Core	
Theory / Practical / Composite: Theory	
No of Modules: Nil	

Course Overview: Algebra-6 and Mathematical Cryptography: This course develops advanced tools in algebra like group actions and analyzing group structures through Sylow Theorems, direct products, semi-direct products etc. In this course one learns about class of simple groups. Also, this introduces field extension, constructions of fields. It also introduces number theory. It also introduces cryptography. Develops algorithms for prime factorization, prime detection.

Course Outcome: On successful completion of the course a student will be able to do the following:

1. **Apply** concepts of group actions, representations, stabilizers, kernels, conjugacy and class equations.
2. **Analyze** finite groups using Sylow theory, simplicity, characteristic and commutator subgroups, composition series and solvability.
3. **Analyze** group products, finite abelian groups and field extensions, and apply these concepts to finite-field construction
4. **Apply** number-theoretic concepts to discrete logarithms and public-key cryptographic protocols.
5. **Analyze and apply** cryptographic algorithms, primality and factorization methods, quadratic-residue theory and pseudo-random number generation.

Prerequisites: Group Theory up to isomorphism theorems.

SYLLABUS

UNIT/Module	CONTENT	NO OF CLASSES	CO Mapping	COGNITIVE LEVEL
I.	Group actions, stabilizers and kernels, permutation representation associated with a given group action, Index theorem. [3] Applications of group actions. Generalized Cayley's theorem. [2] Groups acting on themselves by conjugation, class equation and consequences, conjugacy in Sn [2]	**24**	**CO1, CO2**	**K2, K3, K4**

	p-groups, Sylow's theorems and consequences, Cauchy's theorem [3] Simplicity of An for n ≥ 5, non-simplicity tests. [3] Characteristic subgroups, Commutator subgroup and its properties [3] Composition series, Jordan-Holder Theorem, [3] Solvable groups [2] The group of units modulo n as an external direct product, internal direct products, Fundamental theorem of finite abelian groups. [3]			
II.	Field Extension, Algebraic and Transcendental elements, minimal polynomial of an algebraic element over a field, Degree of an extension, [3] Algebraic and Transcendental Extension, [Any finite extension is any algebraic extension], [3] primitive element for an extension, simple extension, Intermediate Field.[3] Construction of finite fields.[2]	**11**	**CO3**	**K4, K5**
III.	Linear Diophantine Equation, Euler's φ-function [3] Discrete Logarithm problems: Diffe-Hellman key exchange, Elgamal public key encryption, Chinese remainder theorem, Pohlig-Hellman Algorithm [3] RSA, Introduction to Private key encryption, Polard's rho-1 algorithm, Factorization via difference of squares, Primality testing, Miller-Rabin test, generating random primes, [3] Algorithms for factorizing. quadratic sieves, sieve of Eratosthenes. [3] Quadratic residue, Legendre symbol, Quadratic reciprocity, Pseudo-random number generator BBS algorithm. [5]	**17**	**CO4, CO5**	**K2, K3, K4, K5**
Text Books/ Suggested Readings				

1. Algebra: Abstract Algebra, Dummit and Foote. 2. Cryptography: An introduction to Mathematical cryptography, J. Hoffstein, Jill Pipher, Joseph Silverman.
Web Resources and eLearning Sources: MIT OCW 18.702 + Judson + Socratica, Judson + SageMath in CoCalc, Hoffstein–Pipher–Silverman + CryptoHack, Boneh Crypto I + Crandall–Pomerance + SageMath, Hoffstein text + Khan Academy + Wolfram Alpha.
Evaluation: Theory CIA: **20+5+5=30** Semester Exam: **70**
Paper Structure for Theory Semester Exam Module: 7 questions each of **10** marks out of a set of **13** questions.

Course outcomes (COs) and Cognitive Level Mapping

COs	CO Description	Cognitive levels
CO1	**Apply** concepts of group actions, representations, stabilizers, kernels, conjugacy and class equations.	**K2, K3, K4**
CO2	**Analyze** finite groups using Sylow theory, simplicity, characteristic and commutator subgroups, composition series and solvability.	**K2, K3, K4**
CO3	**Analyze** group products, finite abelian groups and field extensions, and apply these concepts to finite-field construction	**K4, K5**
CO4	**Apply** number-theoretic concepts to discrete logarithms and public-key cryptographic protocols.	**K2, K3, K4, K5**
CO5	**Analyze and apply** cryptographic algorithms, primality and factorization methods, quadratic-residue theory and pseudo-random number generation.	**K2, K3, K4, K5**