Faculty of Health, Science and Technology
Mathematics

Syllabus

Algebraic structures, codes and cryptosystems

Course Code:	MAGC15
Course Title:	Algebraic structures, codes and cryptosystems *Algebraiska strukturer, koder och krypton*
Credits:	7.5
Degree Level:	Undergraduate level
Progressive Specialisation:	First cycle, has at least 60 credits in first-cycle course/s as entry requirements (G2F)

Major Field of Study:
MAA (Mathematics)

Course Approval
The syllabus was approved by the Faculty of Health, Science and Technology 2017-08-28, and is valid from the Spring semester 2018 at Karlstad University.

Prerequisites
Mathematics, 60 ECTS cr with at least 45 credits completed, incl MAGA04 Linear algebra, 7,5 ECTS cr, or equivalent

Learning Outcomes
Upon completion of the course the student should be able to:

- define and apply the fundamental concepts and methods in the theories of groups, rings and fields
- analyse the properties of finite groups, determine subgroups and quotient groups
- determine the isomorphism classes of finite groups of low order
- crypt and encrypt a message in RSA encryption
- determine length, dimension and code distance for linear, cyclic and BCH codes
- formulate and apply the theorems of the course
- prove a given subset of the theorems of the course
- show understanding of the subject by demonstrating ability to combine concepts, theorems and examples and ability to discover analogies and make generalizations
- give an account of independently solved mathematical problems, orally and in writing.

Content
Theories of groups: subgroups, cosets and Lagrange's theorem, quotient groups, isomorphisms and homomorphisms, the structure theorem of Abelian groups, the classification of isomorphism, classes of groups of low order, group actions on sets, Sylow's theorems

Theories of rings: characteristics, integral domains, polynomial rings, ideals and quotient rings, ring homomorphisms, the isomorphism theorems, prime and maximal ideals, Euclidean rings, Gaussian

integers

Theories of fields: field extensions, finite fields and number fields

Cryptography: symmetric encryption (secret keys) and asymmetric encryption (public keys), Revest-Shamir-Adelman (RSA) encryption

Error control coding: cyclic codes and BCH codes, perfect codes, encoding and decoding.

Each student is required to carry out a minor project.

Reading List
See separate document.

Examination
Assessment is based on a written exam and a written and oral presentation of the project. The number of retakes for passing the course is limited to three per academic year.

Grades
One of the grades U (Fail), G (Pass), or VG (Distinction) is awarded in the examination of the course.

Quality Assurance
Follow-up relating to learning conditions and goal-fulfilment takes place both during and upon completion of the course in order to ensure continuous improvement. Course evaluation is partly based on student views and experiences obtained in accordance with current regulations and partly on other data and documentation. Students will be informed of the result of the evaluation and of any measures to be taken.

Course Certificate
A course certificate will be provided upon request.

Additional information
The local regulations for studies at the Bachelor and Master levels at Karlstad University stipulate the obligations and rights of students and staff.