Kryptering 1

Cryptography 1

8 ECTS credit points (8 högskolepoäng)

Course code: MA1473
Educational level: Basic level
Course level: G1F
Field of education: Natural sciences
Subject group: Mathematics

1 Course title and credit points
The course is titled Cryptography 1/Kryptering 1 and awards 8 ECTS credits. One credit point (högskolepoäng) corresponds to one credit point in the European Credit Transfer System (ECTS).

2 Decision and approval
This course is established by 2015-03-03. The course syllabus was revised by Head of Department of Mathematics and Natural Science and applies from 2015-03-03.

3 Objectives

4 Content
The course covers the following topics.
• Terminology and problems in cryptology.
• Elementary number theory: advanced congruence theory, modular power calculation, Euler's phi function, primitive roots, and discrete logarithms.
• Modular matrix arithmetics, determinants, and matrix inverse.
• Prime tests: Fermat's and Miller-Rabin's methods.
• Integer factorization: Fermat's method and Pollard's p – 1 method.
• Different types of cryptosystems: symmetric, asymmetric, stream cipher, and block cipher.
• Classical cryptosystems: substitution, affine, Vigenère, Hill, Playfair, ADFGVX, Enigma, and one time pad.
• Modern cryptosystems: Data Encryption Standard (DES), RSA, Cayley-Purser, and ElGamal.
• Cryptanalysis of classical cryptosystems and basic attacks on modern cryptosystems.
• Protocoll: key exchange, digital signature, and flipping coin.
• Mathematical software and mathematical programming.

5 Aims and learning outcomes

Knowledge and understanding
After completion of the course the student will be able to account for
• general terminology and problems in cryptology
• basic concepts in elementary number theory
• bases of different encryption methods and protocols
• weaknesses and strengths of different encryption methods.

Skills and abilities
After completion of the course the student will be able to
• solve linear congruences and apply the Chinese remainder theorem
• formulate and solve problems in modular matrix arithmetics
• compute Euler's phi function
• compute discrete logarithms
• proof results of basic character in elementary number theory
• use algorithms for prime tests or integer factorization
• implement classical and modern cryptosystems and security protocols
• implement a forced attack on a classical cryptosystems.

Judgement and approach
After completion of the course the student will be able to
• that in written and oral communication formulate and motivate various methods of problem solving
• critically read a mathematical text, such as a solution or a proof
• search and retrieve information within the course area of knowledge and prepare a short report under allotted report form with proper referencing.

6 Learning and teaching
Teaching consists of lectures and exercises. The mandatory project assignment can be solved individually or in groups. Oral and written
communication is trained and examined in the project assignment as the student produce their own texts.
The teaching language is Swedish.

7 Assessment and grading

Examination of the course

<table>
<thead>
<tr>
<th>Code</th>
<th>Module</th>
<th>Credit</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1510</td>
<td>Written Examination</td>
<td>4 ECTS</td>
<td>A-F</td>
</tr>
<tr>
<td>1520</td>
<td>Project</td>
<td>3.5 ECTS</td>
<td>G-U</td>
</tr>
<tr>
<td>1530</td>
<td>Write Exercise</td>
<td>0.5 ECTS</td>
<td>G-U</td>
</tr>
</tbody>
</table>

1 Determines the final grade for the course, which will only be issued when all components have been approved. The course will be graded A Excellent, B Very good, C Good, D Satisfactory, E Sufficient, FX Insufficient, supplementation required, F Fail. At grade FX given in consultation with the instructor/examiner opportunity to within 6 weeks of complete score to E for the relevant part of the course.

8 Course evaluation

The course coordinator is responsible for systematically gathering feedback from the students in course evaluations and making sure that the results of these feedback into the development of the course.

9 Prerequisites

Completed courses in Discrete mathematics and Mathematical statistics.

10 Field of education and subject area

The course is part of the field of education and is included in the subject area Mathematics.

11 Restrictions regarding degree

The course cannot form part of a degree with another course, the content of which completely or partly corresponds with the contents of this course.

12 Course literature and other teaching material

Materials distributed by the department.

Reference literature: