

COURSE SYLLABUS AND COURSE REQUIREMENTS

ACADEMIC YEAR 2023/24 SEMESTER SPRING

<i>Course title</i>	<i>Introduction to Computer Science</i>
<i>Subject Code</i>	IVB014ANMI, IVB365ANMI
<i>Hours/Week: le/pr/lab</i>	2/0/0
<i>Credits</i>	3
<i>Degree Programme</i>	Computer Science Engineer
<i>Study Mode</i>	Full time
<i>Requirements</i>	exam
<i>Teaching Period</i>	spring
<i>Prerequisites</i>	No prerequisites
<i>Department(s)</i>	Department of Engineering Mathematics
<i>Course Director</i>	Ákos PILGERMÁJER
<i>Teaching Staff</i>	Ákos PILGERMÁJER

COURSE DESCRIPTION

Concept of numerals, Axioms of Peano, positional numeral systems, arithmetic on positional numeral systems, division, Euclidean algorithm, greatest common divisor (GCD), least common multiple (LCM), extended Euclidean algorithm, number of divisors, prime numbers, irreducible numbers, fundamental theorem of arithmetic, congruencies modulo n , modular arithmetic, congruence or residue classes, complete and reduced residue classes, Euler-Fermat theorem, Euler's totient function, linear congruence systems, Chinese remainder theorem, cryptography, RSA encryption

SYLLABUS

1. GOALS AND OBJECTIVES

The main goal of this course is to making students capable of building and handling RSA cryptosystems. To this end students must understand basic and specific problems and theorems of number theory and be able to apply them to cryptography.

2. COURSE CONTENT

TOPICS

LECTURE	1. Elements of Number Theory 2. Elements of Cryptography
PRACTICE	Not available
LABORATORY	Not available
PRACTICE	

DETAILED SYLLABUS AND COURSE SCHEDULE

LECTURE

<i>week</i>	Topic	Compulsory reading	Required tasks	Completion date, due date
1.	Introductory example of cryptography	[1] Lesson 1	HW 1	Next Friday
2.	Divisibility	[1] Lesson 2	HW 2	Next Friday
3.	Numeral systems, algorithms	[1] Lesson 3	HW 3	Next Friday

4.	Mathematical induction	[1] Lesson 4	HW 4	Next Friday
5.	Representation of numbers	[1] Lesson 5	HW 5	Next Friday
6.	Euclidean algorithm	[1] Lesson 6	HW 6	End of week
7.	First midterm test (MTT1)		MTT 1	In class
8.	Recurring algorithms	[1] Lesson 7	HW 7	Next Friday
9.	Spring break			
10.	Diophantine equations	[1] Lesson 8	HW 8	Next Friday
11.	Congruencies	[1] Lesson 9	HW 9	Next Friday
12.	Chinese remainder theorem	[1] Lesson 10	HW 10	Next Friday
13.	RSA revisited	[1] Lesson 11	HW 11	End of week
14.	Second midterm test MTT2		MTT2	In class

3. ASSESSMENT AND EVALUATION

ATTENDANCE

Method for monitoring attendance

Attendance sheet/ online test/ other valid means of checking attendance. Making up any absence is not possible according to the current state of science. No need for verification of absence, but keep it under the regulation limit (30 % of total contact hours (lectures and laboratory classes)).

ASSESSMENT

Course-unit with final examination

Mid-term assessments, performance evaluation and their weighting as a pre-requisite for taking the final exam

Type	Assessment	Weighting as a proportion of the pre-requisite for taking the exam
1. MidTerm Test 1 (MTT1)	points	40 %
2. MidTerm Test 2 (MTT2)	points	40 %
3. HomeWorks (HWs)	points	20 %
4. Evaluation of class work	points	+10%

Requirements for the end-of-semester signature

- Attendance prescribed by Code of Studies and Examinations (Art. 45. (2)) - no make ups are possible
- Midterm tests: minimum 40% each - make up for at most one test is possible, see below at retakes
- Homeworks turned in until deadline (no delays) with non zero points - during availability continuous make ups are possible
- At least 40% of overall performance calculated from the table above.

Re-takes for the end-of-semester signature

In case the student missed at most one MTT or any of the MTTs are unsuccessful, in the first week of exam period, planned in time of class, can make it up, or retake it, them once.

Type of examination (written, oral): written in Möbius

The exam is successful if the result is minimum 40%.

Calculation of the final grade

- **Offered grade** (without an exam): in case the mid-term performance is at least 55% (in Neptun student must accept or deny it!),
- **Final grade** (with an exam): in case the student cannot earn the offered grade or does not accept it, then must take an exam. In this case the mid-term performance accounts for **50%**, the performance at the exam accounts for **50%** in the calculation of the final grade.

Calculation of the final grade based on aggregate performance in percentage.

Course grade	Performance in %
excellent (5)	85 % ...
good (4)	70 % ... 85 %
satisfactory (3)	55 % ... 70 %
pass (2)	40 % ... 55 %
fail (1)	below 40 %

The lower limit given at each grade belongs to that grade.

4. SPECIFIED LITERATURE

COMPULSORY READING AND AVAILABILITY

[M] lessons in Möbius system

[LLM] Eric Lehman, Frank Thomson Leighton, Albert R. Meyer, *6.042J / 18.062J Mathematics for Computer Science (Spring 2015)*, [Open Courseware MIT](#), [Privacy and Terms of Use](#)

RECOMMENDED LITERATURE AND AVAILABILITY

[ET] Moodle and Teams course materials