<table>
<tr><td>COURSE NAME</td><td colspan="5">Mathematical Fundamentals of Cryptography</td></tr>
<tr><td>Code</td><td>PMM850</td><td>Year of study</td><td colspan="4">1st or 2nd year of graduate study</td></tr>
<tr><td>Course teacher</td><td>Borka Jadrijević</td><td>Credits (ECTS)</td><td colspan="4">5</td></tr>
<tr><td rowspan="2">Associate teachers</td><td rowspan="2"></td><td rowspan="2">Type of instruction (number of hours)</td><td>L</td><td>S</td><td>E</td><td></td></tr>
<tr><td>30</td><td></td><td>30</td><td></td></tr>
<tr><td>Status of the course</td><td>elective course</td><td>Percentage of application of e-learning</td><td colspan="4">40%</td></tr>
<tr><td colspan="6">COURSE DESCRIPTION</td></tr>
<tr><td>Course objectives</td><td colspan="5">The objective of this course is to introduce students of informatics to the mathematical background, basic ideas, techniques and algorithms used in cryptography and its applications. The course provides a good background for understanding and learning more advanced courses in this area.</td></tr>
<tr><td>Prerequisites</td><td colspan="5">No prerequisites</td></tr>
<tr><td>Learning outcomes expected at the level of the course (4 to 10 learning outcomes)</td><td colspan="5">Upon successful completion of the course, the student is able to:
- define the basic mathematical concepts used in cryptography;
- decrypt messages encrypted using the different types of substitution ciphers and columnar transposition;
- describe the basic steps in modern block cryptosystems DES and AES;
- describe the idea of public-key cryptography;
- define RSA cryptosystem and its connection with factorization of large integers;
- encrypt messages using public-key cryptosystems (RSA, Rabin, ElGamal, Merkle-Hellman);
- cryptoanalyze RSA cryptosystem with small public or secret exponent;
- define elliptic curve and describe the use of elliptic curves in cryptography;
- describe the most famous algorithms for primality testing and integral factorization;
- define hash function and describe the idea of digital signature.</td></tr>
<tr><td>Course content broken down in detail by weekly class schedule (syllabus)</td><td colspan="5">Overview of Cryptography: Basic concepts and terminology. (2 hours)
-Mathematical background:
Number theory: Divisibility. Prime numbers. Congruences. Quadratic residues. Diophantine approximation and equations (continued fractions). Basic algorithms in number theory and their complexity. (7 hours)
Algebra: Groups. Rings and fields. Finite fields. (3 hours)
-Some Classical cryptosystems: Basic notions. Caesar, Affine, Vigenère, Playfair and Hill's cipher. Statistical methods for cryptanalysis. Columnar transposition. (4 hours)
- Modern Block Ciphers: Data Encryption Standard (DES). Advanced Encryption Standard (AES). (3 hours)
- Public-Key Cryptography and mathematical problems on which it is based: Concept of public-key cryptography. RSA cryptosystem (primality testing and integral factorization) Diffie–Hellman key exchang and Elgamal's cryptosystem (discrete logarithm problem). Other public-key cryptosystems: Rabin cryptosystem (quadratic residuosity problem), Merkle–Hellman cryptosystem (knapsack problem). Elliptic curves in cryptography. (10 hours)
- Cryptography in practice: Hash functions. Digital signature. Identity problem. (2</td></tr>
</table>

	hours)
Format of instruction	Lectures, tutorial sessions
Student responsibilities	Attendance of lectures and tutorial sessions is obligatory. Students should solve the homework assignments and present a project.
Screening student work *(name the proportion of ECTS credits for each activity so that the total number of ECTS credits is equal to the ECTS value of the course)*	Attendance at lectures and tutorial sessions (1 ECTS) Homeworks (1,5 ECTS) Project (1 ECTS) Oral exam (1,5 ECTS)
Grading and evaluating student work in class and at the final exam	Successful presentation of a project and solving homework assignments are prerequisites for the oral exam. All parts of the exam are equally weighted in the final grade.
Required literature (available in the library and via other media)	1. A.Dujella, M. Maretić: *Kriptogrfija*, Element, Zagreb, 2007.; 2. D A.Dujella, *Diskretna matematika*, skripta, PMF-Matematički odjel, Zagreb, 2004. https://web.math.pmf.unizg.hr/~duje/diskretna/diskretna.pdf 3. K. Ruohonen: *Mathematical Cryptology,* Lecture Notes, http://math.tut.fi/~ruohonen/MC.pdf
Optional literature (at the time of submission of study programme proposal)	1. N. Smart: *Cryptography. An Introduction*, McGraw-Hill, New York, 2002; 2. 2.D. R. Stinson: *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2002.
Quality assurance methods that ensure the acquisition of exit competences	Statistics of test results and anonymous student evaluations at the end of the semester according to the regulations of the University of Split.
Other (as the proposer wishes to add)	