<table>
<tr><td>COURSE NAME</td><td colspan="5">Cryptography</td></tr>
<tr><td>Code</td><td>PMM205</td><td>Year of study</td><td colspan="3">1st and 2nd year of graduate study</td></tr>
<tr><td>Course teacher</td><td>Borka Jadrijević</td><td>Credits (ECTS)</td><td colspan="3">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></tr>
<tr><td>30</td><td>15</td><td>15</td></tr>
<tr><td>Status of the course</td><td>compulsory and elective course</td><td>Percentage of application of e-learning</td><td colspan="3">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 to the basic ideas, techniques and algorithms used in cryptography and its applications. The course is a good background for understanding and learning more advanced courses in this area.</td></tr>
<tr><td>Prerequisites</td><td colspan="5">Completed course: Introduction to number theory</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:
- 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 ideas of public-key cryptography and digital signature;
- 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;
- define notions of (Euler, strong) pseudoprime numbers and determine whether an integer is a pseudoprime;
- describe the most famous algorithms for primality testing and integral factorization.</td></tr>
<tr><td>Course content broken down in detail by weekly class schedule (syllabus)</td><td colspan="5">- Traditional ciphers. Basic notions. Caesar, Vigenère, Playfair and Hill's cipher. Statistical methods for cryptanalysis. Encryption devices. (7 hours)
- Modern Block Ciphers. Data Encryption Standard (DES). Cryptanalysis of DES. Advanced Encryption Standard (AES). (6 hours)
- Public-Key Cryptography. Concept of public-key cryptography. Digital signature. RSA cryptosystem. Other public-key cryptosystems. Cryptanalysis of public-key cryptosystem. Elliptic curves in cryptography. (9 hours)
- Primality Testing and Integral factorization. Pseudoprime numbers. Soloway-Strassen and Miller–Rabin primality test. Factor base. Continued fraction factorization method. Quadratic sieve factoring algorithm. (8 hours)</td></tr>
<tr><td>Format of instruction</td><td colspan="5">Lectures, tutorial sessions, seminars</td></tr>
<tr><td>Student responsibilities</td><td colspan="5">Attendance of lectures and tutorial sessions is obligatory. Students should present a seminar and solve the homework assignments.</td></tr>
<tr><td>Screening student work (name the proportion of ECTS credits for each</td><td colspan="5">Class attendance (1 ECTS)
Homework assignments (1,5 ECTS)
Seminar (1 ECTS)
Oral exam (1,5 ECTS)</td></tr>
</table>

activity so that the total number of ECTS credits is equal to the ECTS value of the course)	
Grading and evaluating student work in class and at the final exam	Successful seminar and success in 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)	A.Dujella, M. Maretić: *Kriptogrfija*, Element, Zagreb, 2007.; D. R. Stinson: *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2002. N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1994.
Optional literature (at the time of submission of study program proposal)	N. Smart: *Cryptography. An Introduction*, McGraw-Hill, New York, 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)	