COURSE NAME Mathematical Fundamentals of Cryptography					
PMM850	Year of study	1st or 2nd year of graduate study			
Borka Jadrijević	Credits (ECTS)	5			
	Type of instruction (number of hours)	L 30	S	E 30	
elective course	Percentage of application of e-learning	40%		1	
COURSE DESCRIPTION					
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.					
No prerequisites					
 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. 					
 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 					
	PMM850 Borka Jadrijević elective course The objective of this course mathematical background, cryptography and its applica understanding and learning No prerequisites Upon successful completion - define the basic ma - decrypt messages of ciphers and column - describe the basic s - describe the basic s - describe the idea of - define RSA cryptos integers; - encrypt messages of Merkle-Hellman); - cryptoanalyze RSA - define elliptic curve - describe the most fr factorization; - define hash function Overview of Cryptography -Mathematical background Number theory: Divisibility Diophantine approximation number theory and their cor Algebra: Groups. Rings and -Some Classical cryptosy and Hill's cipher. Statistical hours) - Public-Key Cryptograph Concept of public-key cry integral factorization) Diffe (discrete logarithm problem (quadratic residuosity proble	PMM850 Year of study Borka Jadrijević Credits (ECTS) Type of instruction (number of hours) Type of instruction (number of hours) elective course Percentage of application of e-learning COURSE DESCRIPTION The objective of this course is to introduce students of mathematical background, basic ideas, techniques a cryptography and its applications. The course provide understanding and learning more advanced courses i No prerequisites Upon successful completion of the course, the studer - define the basic mathematical concepts used - decrypt messages encrypted using the differe ciphers and columnar transposition; - describe the idea of public-key cryptography; - define RSA cryptosystem and its connection - integers; - encrypt messages using public-key cryptosystem Merkle-Hellman); - cryptoanalyze RSA cryptosystem with small p - define elliptic curve and describe the use of e - describe the most famous algorithms for prim factorization; - define hash function and describe the idea of Overview of Cryptography: Basic concepts and terr - Mathematical background: Number theory and their complexity. (7 hours) Algebra: Groups. Rings and fields. Finite fields. (3 ho - Some Classical cryptosystems: Basic notions. Ca and Hill's cipher. Statistical methods for cryptanalys hours) - Modern Block Ciphers: Data Encryption Standard (AES). (3 hours) - Public-Key Cryptography and mathematical pro Concept of public-key cryptography. RSA cryptog integral factorization) Diffie-Hellman key exchang (discrete logarithm problem). Other public-key cryptog integral factorization Diffie-Hellman key exchang integral	PMM850 Year of study 1st or study Borka Jadrijević Credits (ECTS) 5 Type of instruction (number of hours) 10 elective course Percentage of application of e-learning 40% COURSE DESCRIPTION The objective of this course is to introduce students of inform: mathematical background, basic ideas, techniques and algor cryptography and its applications. The course provides a good understanding and learning more advanced courses in this ar No prerequisites Upon successful completion of the course, the student is able - define the basic mathematical concepts used in crypt - decrypt messages encrypted using the different types ciphers and columnar transposition; - describe the basic steps in modern block cryptosystem - describe the idea of public-key cryptography; - define RSA cryptosystem and its connection with fact integers; - encrypt messages using public-key cryptosystems (R Merkle-Hellman); - cryptoanalyze RSA cryptosystem with small public or - define elliptic curve and describe the use of elliptic cu - describe the most famous algorithms for primality tes factorization; - define hash function and describe the idea of digital s Overview of Cryptography: Basic concepts and terminology. -Mathematical background: Number theory: Divisibility. Prime numbers. Congruences Diophantine approximation and equations (continued fraction number theory and their complexity. (7 hours) Algebra: Groups. Rings and fields. Finite fields. (3 hours) -Some Classical cryptosystems: Basic notions. Caesar, Af and Hill's cipher. Statistical methods for cryptanalysis. Colu hours) - Modern	PMM850 Year of study 1st or 2nd year study Borka Jadrijević Credits (ECTS) 5 Type of instruction (number of hours) 10 30 elective course Percentage of application of e-learning 40% COURSE is to introduce students of informatics to 1 mathematical background, basic ideas, techniques and algorithms us cryptography and its applications. The course provides a good backgr understanding and learning more advanced courses in this area. No prerequisites Upon successful completion of the course, the student is able to: - define the basic mathematical concepts used in cryptography - describe the idea of public-key cryptosystems DES - describe the basic steps in modern block cryptosystems DES - describe the idea of public-key cryptosystems (RSA, Rat Merkle-Hellman); - cryptoanalyze RSA cryptosystem with small public or secret e define elliptic curve and describe the use of elliptic curves in of factorization; - define hash function and describe the idea of digital signature Overview of Cryptography: Basic concepts and terminology. (2 hot Mathematical background: Mathematical background: Number theory: Divisibility. Prime numbers. Congruences. Quadh factorization; - define hash function and describe the idea of digital signature Overview of Cryptography: Basic concepts and terminology. (2 hot Mathematical background: Number theory: Divisibility. Prime numbers. Congruences. Quadh factorization;<	PIMM850 Year of study 1st or 2nd year of gra study Borka Jadrijević Credits (ECTS) 5 Type of instruction (number of hours) 10 30 30 elective course Percentage of application of e-learning 40% COURSE DESCRIPTION 40% 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 fo understanding and learning more advanced courses in this area. No prerequisites 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 idea of public-key cryptography; - define RSA cryptosystem and its connection with factorization of larg integers; - encrypt messages using public-key cryptosystems (RSA, Rabin, ElGi Merkle-Hellman); - cryptoanalyze RSA cryptosystem with small public or secret exponen - define hash function and describe the use of elliptic curves in cryptogr - describe the most famous algorithms for primality testing and integral factorization; - define hash function and describe the idea of digital signature. Overview of Cryptography: Basic concepts and terminology. (2 hours) -Mathematical background: Number theory: Divisibility. Prime numbers. Congruences. Quadratic re Diophantine approximation and equations (continued fractions). Basic algorit number theory and their complexity. (7

	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)	 A.Dujella, M. Maretić: <i>Kriptogrfija</i>, Element, Zagreb, 2007.; D A.Dujella, <i>Diskretna matematika</i>, skripta, PMF-Matematički odjel, Zagreb, 2004. https://web.math.pmf.unizg.hr/~duje/diskretna/diskretna.pdf K. Ruohonen: <i>Mathematical Cryptology</i>, Lecture Notes, http://math.tut.fi/~ruohonen/MC.pdf
Optional literature (at the time of submission of study programme proposal)	 N. Smart: <i>Cryptography. An Introduction</i>, McGraw-Hill, New York, 2002; 2. 2.D. R. Stinson: <i>Cryptography. Theory and Practice</i>, 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)	