<table>
<tr><td>NAZIV PREDMETA</td><td colspan="5">Matematičke osnove kriptografije</td></tr>
<tr><td>Kod</td><td>PMM850</td><td>Godina studija</td><td colspan="4">1. ili 2. godina diplomskog studija</td></tr>
<tr><td>Nositelj/i predmeta</td><td>Borka Jadrijević</td><td>Bodovna vrijednost (ECTS)</td><td colspan="4">5</td></tr>
<tr><td rowspan="2">Suradnici</td><td rowspan="2"></td><td rowspan="2">Način izvođenja nastave (broj sati u semestru)</td><td>P</td><td>S</td><td>V</td><td>T</td></tr>
<tr><td>30</td><td></td><td>30</td><td></td></tr>
<tr><td>Status predmeta</td><td>Izborni</td><td>Postotak primjene e-učenja</td><td colspan="4">40%</td></tr>
<tr><td colspan="6">OPIS PREDMETA</td></tr>
<tr><td>Ciljevi predmeta</td><td colspan="5">Cilj kolegija je upoznati studente informatike s matematičkim pozadinom, osnovnim idejama, tehnikama i algoritmima koji se koriste u kriptografiji i njenoj primjeni. Kolegij je dobar temelj za razumijevanje i učenje naprednijih kolegija iz ovog područja.</td></tr>
<tr><td>Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet</td><td colspan="5">Nema preduvjeta</td></tr>
<tr><td>Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)</td><td colspan="5">Po uspješnom završetku kolegija student može:
- definirati osnovne matematičke pojmove koji se koriste u kriptografiji;
- dekriptirati poruke šifrirane različitim supstitucijskim šiframa te stupčanom transpozicijom;
- objasniti osnovne korake u šifriranju modernim blokovnim kriptosustavima DES i AES;
- objasniti ideju javnog ključa;
- definirati kriptosustav RSA te objasniti njegovu vezu s faktorizacijom velikih prirodnih brojeva;
- šifrirati poruku pomoću najpoznatijih kriptosustava s javnim ključem (RSA, Rabin, ElGamal, Merkle-Hellman);
- kriptoanalizirati RSA kriptosustav s malom duljinom javnog ili tajnog eksponenta;
- definirati eliptičku krivulju i objasniti primjenu eliptičkih krivulja u kriptografiji;
- opisati osnovne algoritme za faktorizaciju te testiranje prostosti.
- definirati hash funkciju i objasniti ideju digitalnog potpisa;</td></tr>
<tr><td>Sadržaj predmeta detaljno razrađen prema satnici nastave</td><td colspan="5">- Pregled kriptografije: Osnovni pojmovi i ideje. (2 sata).

- Matematička pozadina:
Teorija brojeva: Djeljivost. Prosti brojevi. Kongruencije. Kvadratni ostaci. Diofantske aproksimacije i jednadžbe (razvoj u verižni razlomak). Osnovni algoritmi teorije brojeva i njihova složenost. (7 sati)
Algebra: Grupe. Prsteni i polja. Konačna polja. (3 sata)

- Neki klasični kriptosustavi: Cezarova, Afina, Vigenèreova, Hillova šifra. Statističke metode u kriptoanalizi. Stupčana transpozicija. (3 sata)

- Moderni blokovni simetrični kriptosustavi. Data Encryption Standard (DES). Advanced Encryption Standard (AES). (3 sata)

- Kriptosustavi s javnim ključem i matematički problemi na kojima su zasnovani: Ideja javnog ključa. RSA (faktorizacija i testiranje prostosti). Diffie-Hellman protokol za razmjenu ključeva i Elgamalov kriptosustav (problem diskretnog logaritma). Ostali kriptosustavi: Rabinov (problem kavadratnog korijena). Merkle-Hellmanov kriptosustav (problem ruksaka). Eliptičke krivulje u kriptografiji.</td></tr>
</table>

	(10 sati) - **Kriptografija u praksi**: hash funkcije, digitalni potpis, problem identiteta. (2 sata)					
Vrste izvođenja nastave:	☒ predavanja ☒ vježbe					
Obveze studenata	Pohađanje nastave, pisanje domaćih zadaća, prezentacija projekta					
Praćenje rada studenata *(upisati udio u ECTS bodovima za svaku aktivnost tako da ukupni broj ECTS bodova odgovara bodovnoj vrijednosti predmeta):*	Pohađanje nastave	1	Istraživanje		Praktični rad	
	Eksperimentalni rad		Referat		Domaće zadaće	1,5
	Esej		Seminarski rad		(Ostalo upisati)	
	Kolokviji		Usmeni ispit	1,5	(Ostalo upisati)	
	Pismeni ispit		Projekt	1	(Ostalo upisati)	
Ocjenjivanje i vrjednovanje rada studenata tijekom nastave i na završnom ispitu	Uspješno prezentiran projekt te uspjeh u rješavanju domaćih zadaća je uvjet za pristupanje završnom usmenom ispitu. Domaće zadaće i završni usmeni ispit jednako se vrednuju u konačnoj ocjeni.					

	Naslov	**Broj primjeraka u knjižnici**	**Dostupnost putem ostalih medija**
Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	1. A.Dujella, M. Maretić: *Kriptografija*, Element, Zagreb, 2007.;	do 3	
	2.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		
Dopunska literatura	1.N. Smart: *Cryptography. An Introduction*, McGraw-Hill, New York, 2002; 2.D. R. Stinson: *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 2002.		
Načini praćenja kvalitete koji osiguravaju stjecanje utvrđenih ishoda učenja	Statistika ispitnih rezultata i studentsko vrednovanje putem anonimne ankete na kraju izvedbe predmeta. Anketa se provodi prema pravilniku Sveučilišta u Splitu.		
Ostalo (prema mišljenju predlagatelja)			