<table>
<tr><td>NAZIV PREDMETA</td><td colspan="5">Kriptografija</td></tr>
<tr><td>Kod</td><td>PMM205</td><td>Godina studija</td><td colspan="4">2.</td></tr>
<tr><td>Nositelj/i predmeta</td><td>izv. prof.dr.sc. Borka Jadrijević</td><td>Bodovna vrijednost (ECTS)</td><td colspan="4">5,0</td></tr>
<tr><td rowspan="2">Suradnici</td><td rowspan="2">Marija Bliznac, mag. math.</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>15</td><td>15</td><td></td></tr>
<tr><td>Status predmeta</td><td>obavezan</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 s 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">Položen kolegij: Uvod u teoriju brojeva</td></tr>
<tr><td>Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)</td><td colspan="5">Po uspješnom završetku kolegija student može: - dekriptirati poruke šifrirane različitim supstitucijskim šiframa te stupčanom transpozicijom; - objasniti osnovne korake u šifriranju modernim blokovnim kriptosustavima DES i AES; - objasniti ideju javnog ključa i digitalnog potpisa; - 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; - definirati pojam (Eulerovog, jakog) pseudoprostog broja te za konkretni prirodni broj znati provjeriti je li pseudoprost; - opisati osnovne algoritme za faktorizaciju te testiranje prostosti.</td></tr>
<tr><td>Sadržaj predmeta detaljno razrađen prema satnici nastave</td><td colspan="5">- Klasična kriptografija. Osnovni pojmovi. Cezarova, Vigenèreova, Playfairova i Hillova šifra. Statističke metode u kriptoanalizi. Naprave za šifriranje. (7 sati) - Moderni blokovni simetrični kriptosustavi. Data Encryption Standard (DES). Kriptoanaliza DES-a. Advanced Encryption Standard (AES). (6 sati) - Kriptografija javnog ključa. Ideja javnog ključa. Digitalni potpis. RSA kriptosustav. Ostali kriptosustavi s javnim ključem. Kriptoanaliza kriptosustava s javnim ključem. Eliptičke krivulje u kriptografiji. (9 sati) - Testovi prostosti i metode faktorizacije. Pseudoprosti brojevi. Soloway-Strassenov i Miller-Rabinov test prostosti. Faktorske baze. Faktorizacija metodom verižnog razlomka. Metoda kvadratnog sita. (8 sati)</td></tr>
<tr><td>Vrste izvođenja nastave:</td><td colspan="5">predavanja, seminari, vježbe</td></tr>
<tr><td>Obveze studenata</td><td colspan="5">Pohađanje nastave, pisanje domaćih zadaća i izrada seminarskog rada</td></tr>
</table>

Praćenje rada studenata *(upisati udio u ECTS bodovima za svaku aktivnost tako da ukupni broj ECTS bodova odgovara bodovnoj vrijednosti predmeta):*	Pohađanje nastave 1 ECTS Seminarski rad 1 ECTS Usmeni ispit 1,5 ECTS Domaće zadaće 1,5 ECTS
Ocjenjivanje i vrjednovanje rada studenata tijekom nastave i na završnom ispitu	Uspješno održan seminar te uspjeh u rješavanju domaćih zadaća je uvjet za pristupanje završnom usmenom ispitu. Domaće zadaće, seminarski rad i završni usmeni ispit jednako se vrednuju u konačnoj ocjeni.
Obvezna literatura (dostupna u knjižnici i putem ostalih medija)	
	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.
Dopunska literatura	N. Smart: Cryptography. An Introduction, McGraw-Hill, New York, 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)	