NAZIV PREDMETA	KRIPTOGRAFIJA S PRIMJENOM					
Kod	DET038	Godina studija	2.			
Nositelj/i predmeta	Mr.sc. Tonko Kovačević, viši predavač	Bodovna vrijednost (ECTS)	6			
Suradnici		Način izvođenja nastave (broj sati u semestru)	P	S	V	T
			30		30	
Status predmeta	Izborni	Postotak primjene e-učenja	40%			

OPIS PREDMETA

Ciljevi predmeta	• Usvajanje znanja iz područja kriptografije • Primjena kriptografskih sustava za zaštitu podataka i resursa u informacijskim i komunikacijskim sustavima
Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet	Nema
Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)	1. Analizirati kriptografske sustave 2. Dizajnirati i realizirati sigurne komunikacijske sustave 3. Primijeniti kriptografske sustave u različitim aplikacijama 4. Odabrati inženjerski pristup u nadzoru sigurnosti komunikacijskih sustava polazeći od usvojenih teorijskih i praktičnih znanja

Sadržaj predmeta detaljno razrađen prema satnici nastave

Tjedan	Sati	Oblik nastave	Tema
1.	2	Predavanja	Uvod u informacijsku sigurnost i kriptografiju i osnovne sigurnosne prijetnje
	2	Laboratorijske vježbe	Upoznavanje s Matlab funkcijama za primjenu u kriptografiji
2.	*2*	Predavanja	Supstitucijske i permutacijske šifre, Vigenereova šifra, Vernamova šifra i Hillova šifra
	2	Laboratorijske vježbe	Vigenèreova i Hillova šifra
3.	2	Predavanja	Osnovna teorija brojeva
	2	Laboratorijske vježbe	Računanje po modulu, konačna polja i generator slučajnih brojeva
4.	2	Predavanja	DES i AES kriptosustavi
	2	Laboratorijske vježbe	Primjena DES i AES enkripcije
5.	2	Predavanja	Kriptografija javnog ključa
	2	Laboratorijske vježbe	Modovi rada modernih šifri (ECB, CBC, CFB, OFB, CTR mode)
6.	2	Predavanja	RSA kripostustav i Diffie-Hellman protokol za uspostavu tajnog ključa
	2	Laboratorijske vježbe	Primjena RSA algoritma
7.	*2*	Predavanja	Autentifikacijske funkcije (kriptografske „hash“ funkcije i MAC algoritmi)
	2	Laboratorijske	Primjena autentifikacijskih funkcija

			vježbe	
	8.	2	Predavanja	1. kolokvij Digitalni potpis i certifikati
		2	Laboratorijske vježbe	Analiza sigurnosti protokola 1. (Scyther)
	9.	2	Predavanja	IPsec protokol
		2	Laboratorijske vježbe	Analiza sigurnosti protokola 2. (Scyther)
	10.	2	Predavanja	Web sigurnost – SSL/TSL
		2	Laboratorijske vježbe	IPsec konfiguracija
	11.	2	Predavanja	Napredna autentifikacija poruka u bežičnim mrežama
		2	Laboratorijske vježbe	IPsec upravljanje ključevima
	12.	2	Predavanja	Mehanizmi za distribuciju kriptografskih ključeva
		2	Laboratorijske vježbe	SSL/TSL client - server
	13.	2	Predavanja	Primjena kriptografskih sustava u kartičnom i e-poslovanju
		2	Laboratorijske vježbe	E-kartice, zaštita podataka
	14.	2	Predavanja	Primjena kriptografskih sustava u bežičnim mrežama
		2	Laboratorijske vježbe	Konfiguracija sigurnosti u WiFi mreži
	15.	4	dopunski	2. pripreme za ispit, kolokvij, kolokvij - laboratorijske vježbe

Vrste izvođenja nastave:	☒ predavanja ☐ seminari i radionice ☒ vježbe ☐ *on line* u cijelosti ☒ mješovito e-učenje ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija ☒ laboratorij ☐ mentorski rad ☒ demonstracijske vježbe
Obveze studenata	• Obavljanje svih propisanih laboratorijskih vježbi. • Predavanje izvješća s laboratorijskih vježbi.Ocjena laboratorijskih vježbi sastavni je dio ukupne ocjene predmeta. • Nazočnost na predavanjima i auditornim vježbama u iznosu od najmanje 70% predviđene satnice (za izvanredne studente obveza je 50% nazočnosti).	

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	Istraživanje	0,5 ECTS	Praktični rad	1 ECTS
	Eksperimentalni rad		Referat		Demonstracijske vježbe	0,5 ECTS
	Esej		Seminarski rad		Samostalno učenje	1,5 ECTS
	Kolokviji	1ECTS	Usmeni ispit		Konzultacije i završni ispit	0,5 ECTS
	Pismeni ispit		Projekt			

Ocjenjivanje i vrjednovanje rada studenata tijekom nastave i na završnom ispitu

KONTINUIRANA PROCJENA		
Pokazatelji kontinuirane provjere	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Nazočnost i aktivnost na nastavi (predavanja + vježbe)	70 - 100	10
Laboratorijske vježbe	100	10
Laboratorijske vježbe (završna provjera)	50-100	10
Prvi kolokvij	50-100	35
Drugi kolokvij	50-100	35

Studenti koji nisu položili ispit putem kolokvija polažu završni ispit koji se sastoji od praktičnog i teorijskog dijela. Isto vrijedi i za popravne ispite.

ZAVRŠNA PROCJENA		
Pokazatelji provjere - završni ispit (prvi i drugi ispitni termin)	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Praktični ispit (pisani)	50 - 100	40
Teorijski ispit (pisani i/ili usmeni)	50 - 100	50
Prethodne aktivnosti (uključuju sve pokazatelje kontinuirane provjere)	50 - 100	10
Pokazatelji provjere - popravni ispit (treći i četvrti ispitni termin)	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Praktični ispit (pisani)	50 - 100	50
Teorijski ispit (pisani i/ili usmeni)	50 - 100	50

Ocjena (u postotcima) formira se temeljem svih pokazatelja koji opisuju razinu studentskih aktivnosti prema relaciji:

$$Ocjena\ \ (\%) = \sum_{i=1}^{N} k_i A_i$$

k_i- težinski koeficijent za pojedinu aktivnost,
A_i- postotni uspjeh postignut za pojedinu aktivnost,
N - ukupan broj aktivnosti.

ODNOS POLUČENOG USPJEHA I PRIPADNE OCJENE		
Postotak	Kriterij	Ocjena
od 50% do 61%	*zadovoljava minimalne kriterije*	dovoljan (2)
od 62% do 74%	*prosječan uspjeh s primjetnim nedostatcima*	dobar (3)
od 75% do 87%	*iznadprosječan uspjeh s ponekom greškom*	vrlo dobar (4)
od 88% do 100%	*izniman uspjeh*	izvrstan (5)

Obvezna literatura (dostupna u knjižnici i putem	Naslov	Broj primjeraka u knjižnici	Dostupnost putem ostalih medija

ostalih medija)	1. Nastavni materijali (Moodle)		Web izdanje (Moodle)
	2. Vježbe – Materijali (Moodle)		Web izdanje
Dopunska literatura	1. A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007. 2. W. Stallings: Cryptography and Network Security. Principles and Practice, Prentice Hall, 2005.		
Načini praćenja kvalitete koji osiguravaju stjecanje utvrđenih ishoda učenja	• Evidencija pohađanja nastave i uspješnosti izvršenja ostalih obveza studenata (nastavnik). • Ažuriranje detaljnih izvedbenih planova nastave - DIP (nastavnik). • Nadzor izvođenja nastave (zamjenik pročelnika Odjela za nastavu, pročelnici odsjeka). • Kontinuirana provjera kvalitete svih parametara nastavnog procesa u skladu s Akcijskim planovima (pomoćnik pročelnika Odjela za kvalitetu). • Semestralno provođenje studentske ankete sukladno „Pravilniku o postupku studentskog vrednovanja nastavnog rada na sveučilištu u Splitu“ (UNIST, Centar za unaprjeđenje kvalitete).		
Ostalo (prema mišljenju predlagatelja)	DIP-ovi predmeta nalaze se unutar sustava za podršku nastavi (Moodle) i dostupni su studentima i nastavnicima Odjela. Skraćeni izvedbeni programi - IP (hrvatska i engleska inačica) su u cilju javnosti informiranja izravno dostupni na web stranicama Odjela.		