Prirodno-matematički fakultet / Računarske nauke / BEZBJEDNOST RAČUNARSKIH SISTEMA

Uslovljenost drugim predmetima	nema uslovljenosti
Ciljevi izučavanja predmeta	Upoznavanje studenata sa prijetnjama bezbjednosti u računarskim sistemima i načinima, oblicima i metodama zaštite računarskih sistema. Izučavanje algoritama korišćenih za šifriranje informacija. Upoznavanje sa praktičnom primjenom kriptografije u oblasti zaštite računarskih sistema, zaštitom elektronske pošte, web-a i transakcija, kao i savremenom zaštitom na mrežnom nivou.
Ime i prezime nastavnika i saradnika	Prof. dr Stevan Šćepanović - predavanja
Metod nastave i savladanja gradiva	Predavanja i demonstracije u računarskoj učionici / laboratoriji. Učenje i samostalna izrada praktičnih zadataka. Konsultacije.
I nedjelja, pred.	Uvod. Osnovni pojmovi o bezbjednosti u računarskim sistemima.
I nedjelja, vježbe	
II nedjelja, pred.	Prijetnje bezbjednosti u računarskim sistemima i principi izgradnje bezbjednog računarskog sistema.
II nedjelja, vježbe	
III nedjelja, pred.	Degradacija sistema pomoću virusa i drugih štetnih programa. Preventivna zaštita računara od virusa. Antivirus programi.
III nedjelja, vježbe	
IV nedjelja, pred.	Neophodna zaštita računarskih sistema, politika i mehanizmi zaštite. Osnovni pojmovi iz kriptografije i kriptoanalize. Klasifikacija kriptosistema.
IV nedjelja, vježbe	
V nedjelja, pred.	Simetrično ili klasično šifriranje. Apsolutno sigurna šifra. Konfuzija i difuzija i osnovni principi šifriranja. Blokovske šifre. Šifrovanje premještanjem i zamjenom.
V nedjelja, vježbe	
VI nedjelja, pred.	Fajstelova šifra. DES standard šifriranja podataka. Trojno šifrovanje. Otvaranje DES šifri. Ostale simetrične šifre.
VI nedjelja, vježbe	
VII nedjelja, pred.	I Kolokvijum.
VII nedjelja, vježbe	
VIII nedjelja, pred.	AES - napredni standard šifriranja. Rijndael-ova šifra. Pouzdanost korišćenja simetričnih šifri. Lokacija i razmještaj funkcija i uređaja za šifriranje.
VIII nedjelja, vježbe	
IX nedjelja, pred.	Algoritmi sa otvorenim ključevima. Algoritam RSA. Protokoli za provjeru i principi izgradnje protokola autentičnosti. Autentičnost na osnovu dijeljenog ključa.
IX nedjelja, vježbe	
X nedjelja, pred.	Instalacija dijeljenog ključa i Difi-Helmanov protokol za razmjenu ključeva. Provjera originalnosti kroz centar za distribuciju ključeva i Protokol Nidhema-Šredera za provjeru autentičnosti. Utvrđivanje originalnosti protokolom Kerber.
X nedjelja, vježbe	
XI nedjelja, pred.	Elektronski potpis sa tajnim ključem i elektronski potpis sa otvorenim ključem. Hash funkcije. Generacija Message Digest korišćenjem SHA-1. Elektronska uvjerenja. Kontrola pristupa i autorizacija kao mehanizam zaštite.
XI nedjelja, vježbe	
XII nedjelja, pred.	Zaštita elektronske pošte (PGP operacije i zaštitno višenamjensko Internet Mail proširenje - S/MIME). Zaštita Web-a (SSL Protokol i Internet TLS standard). Zaštita elektronskih transakcija.
XII nedjelja, vježbe	
XIII nedjelja, pred.	Zaštita na mrežnom nivou i IP zaštita. Transportni i tunelski režim zaštite, AH i ESP. Virtuelne privatne mreže i tunelovanje. Zaštitna barijera (firewall).
XIII nedjelja, vježbe	
XIV nedjelja, pred.	II Kolokvijum.
XIV nedjelja, vježbe	

XV nedjelja, pred.	Popravni kolokvijum
XV nedjelja, vježbe	
Obaveze studenta u toku nastave	Studenti su obavezni da aktivno prate nastavu, predaju domaće zadatke, rade oba kolokvijuma i urade sve planom predviđene vježbe.
Konsultacije	Svake nedelje poslije predavanja.
Opterećenje studenta u casovima	4 kredita x 30 sati = 120 sati
Literatura	1. M. Strib, Č. Perkins - “Firewalls zaštita od hakera", Kompjuter biblioteka, “Svetlost”, Čačak, 2003. 2. S. McClure, J. Scambray, G. Kurtz - “Sigurnost na mreži”, Kompjuter biblioteka, “Svetlost”, Čačak, 2001. 3. W. Stallings, - “Cryptography and Network Security.", Prentice-Hall, Inc., New Jersey, 1999.
Oblici provjere znanja i ocjenjivanje	Dva kolokvijuma se ocijenjuju ukupno sa 70 poena. Završni ispit 30 poena. Prelazna ocjena se dobija ako se kumulativno sakupi najmanje 50 poena.
Posebne naznake za predmet	
Napomena	
Ishodi učenja	Nakon što student položi ovaj ispit, biće u mogućnosti da: 1.Objasni pojam bezbjednog računarskog sistema. 2.Opiše moguće prijetnje i rizike ugrožavanja bezbjednosti računarskih sistema. 3.Opiše pojmove autentičnosti i autorizacije i protokole za njihovu realizaciju. 4.Ovlada sadržajima koji uključuju šifriranje i dešifriranje podataka, algoritme šifriranja i procedure zaštite. 5.Opiše metodologiju zaštite elektronske pošte, veba, elektronskog potpisa i elektronskog sertifikata. 6.Projektuje i implementira neophodnu zaštitu konkretnog računarskog sistema.