

MI003	Izborni 2. godina	Kriptografija i sigurnost sustava	P	V	S	ECTS 5
			2	2	0	

Cilj predmeta. Upoznati studente s temeljnim pojmovima i metodama klasične i moderne kriptografije. Predstaviti osnovne ideje enkripcije i dekripcije podataka, s posebnim naglaskom na primjeni teorije brojeva u modernoj kriptografiji. Proučiti svojstva kriptosustava, obraditi metode zaštite operacijskih sustava, determinirati njihove prednosti i nedostatke. Ovladati metodama dekripcije pri napadima specifičnog tipa na poznate kriptosustave. Programirati različite enkripcijske i dekripcijske postupke te testirati metode na različitim primjerima.

Potrebna predznanja. Preddiplomski studij matematičkog ili računarskog smjera

Sadržaj predmeta.

1. Kriptografija. Osnovni pojmovi i tipova napada. Podjele kriptosustava. Klasična kriptografija i frekvencijska analiza.
2. Kongruencije u kriptografiji. Osnovna svojstva kongruencija, prosti i pseudoprosti brojevi. Modeliranje, projektiranje i provjera sigurnosnih protokola.
3. Kriptosustavi s javnim ključem. RSA kriptosustav. Generiranje pseudoslučajnih brojeva.
4. Autentifikacija. Digitalni potpis. Infrastruktura javnog ključa i zaštitno upravljanje.
5. Modeli sigurnosnog upravljanja i nadzora. Analiza modela i nepouzdana mjesta u sustavu.
6. Zaštita. Višerazinske sigurnosne baze podataka. Sigurnost i mjere zaštite.

ISHODI UČENJA

R.b.	ISHODI UČENJA
1.	Razlikovati tipove kriptosustava i tipove napada.
2.	Primijeniti svojstva prostih i pseudoprostih brojeva u konstrukciji kriptosustava.
3.	Upotrijebiti kriptosustave s javnim ključem.
4.	Razumijeti i provesti postupak digitalnog potpisivanja.
5.	Identificirati nepouzdana mjesta u sustavu.
6.	Analizirati mjere sigurnosti i postupak zaštite sustava.

POVEZIVANJE ISHODA UČENJA, ORGANIZACIJE NASTAVNOG PROCESA I PROCJENA ISHODA UČENJA

ORGANIZACIJA NASTAVNOG PROCESA	ECTS	ISHOD UČENJA **	AKTIVNOST STUDENATA*	METODA PROCJENE	BODOVI	
					min	max
Pohađanje predavanja	1	1-6	Prisutnost na nastavi, rasprava, timski rad i samostalan rad na zadacima	Potpisne liste, praćenje aktivnosti na nastavi	0	4
Provjera znanja (kolokvij)	2	1-6	Priprema za pismenu provjeru znanja	Provjera točnih odgovora (ocjenjivanje)	25	48
Završni ispit	2	1-6	Ponavljjanje gradiva	Usmeni ispit	25	48
UKUPNO	5				50	100

Izvođenje nastave i vrednovanje znanja. Predavanja i vježbe su obvezne. Ispit se sastoji od pismenog i usmenog dijela, a polaže se nakon odslušanih predavanja i obavljenih vježbi. Prihvatljivi rezultati postignuti na kolokvijima, koje studenti pišu tijekom semestra, zamjenjuju pismeni dio ispita.

Može li se predmet izvoditi na engleskom jeziku: Da

Osnovna literatura:

1. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 2001. (dostupno on-line)
2. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, 1994.

Dopunska literatura:

1. D.R. Stinson, Cryptography. Theory and Practice, CRC Press, Boca Raton, 2002.
2. B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons Inc., 2000.
3. A. Dujella, M. Maretić: Kriptografija, Element, Zagreb, 2007.