I004	Izborni 5. godina	**Kriptografija i sigurnost sustava**	P+V+S 2+2+0	ECTS 6

Cilj predmeta. Cilj ovog predmeta je upoznati studente s temeljnim pojmovima i metodama kriptografije i zaštite računalnih sustava. Studentima će biti predstavljene osnovne ideje enkripcije i dekripcije podataka te će biti upoznati s višekorisničkim i višezadaćnim operacijskim sustavima. Na predavanjima će se uvoditi i obrađivati pojmovi iz kriptografije i zaštite operacijskih sustava, pri čemu će se proučavati njihova svojstva, prednosti i nedostatci. Na vježbama će studenti upoznavati i programirati različite enkripcijske i dekripcijske postupke te svladavati tehnike analiziranja sigurnosti operacijskih sustava i baza podataka.

Potrebna predznanja. Preddiplomski studij matematike.

Sadržaj predmeta.
1. Kriptografija. Kongruencije u kriptografiji. Osnovna svojstva kongruencija, Eulerov teorem, prosti i pseudoprosti brojevi. Modeliranje, projektiranje i provjera sigurnosnih protokola.
2. Enkripcija i dekripcija podataka. Kriptosustavi. RSA kriptosustav. Kriptosustavi s javnim ključem. Generiranje pseudoslučajnih brojeva.
3. Autentifikacija. Digitalni potpis. Infrastruktura javnog ključa i zaštitno upravljanje.
4. Modeli sigurnosnog upravljanja i nadzora. Analiza modela i nepouzdana mjesta u sustavu.
5. Zaštita. Višerazinske sigurnosne baze podataka. Sigurnost mreže i mjere zaštite. Sigurnosne brane i zastupnički poslužitelji.

Očekivani ishodi učenja.
Očekuje se da nakon položenog kolegija studenti:
- razlikuju kriptosustave;
- razumiju važnost i ulogu kongruencija, prostih i pseudoprostih brojeva u kriptosustavima;
- interpretiraju i koriste postupak enkripcije i dekripcije podataka u osnovnim kriptosustavima;
- provode postupak autentifikacije i provjere digitalnog potpisa;
- analiziraju nepouzdana mjesta u sustavu;
- ilustriraju mjere sigurnosti i postupak zaštite.

Izvođenje nastave i vrednovanje znanja.
Predavanja i vježbe su obavezni. Ispit se sastoji od pismenog i usmenog dijela, a polaže se nakon odslušanih predavanja. Prihvatljivi rezultati postignuti na kolokvijima, koje studenti pišu tijekom semestra, zamjenjuju pismeni dio ispita. Studenti mogu utjecati na ocjenu tako da tijekom semestra pišu domaće zadaće ili izrade seminarski rad.

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, Applied Cryptography: Protocols, Algorithms and Source Codes in C, John Wiley & Sons Inc. 1995
3. B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons Inc. 2000