Studijski program: STUDIJE I CIKLUSA - INFORMACIONE TEHNOLOGIJE - 240 ECTS			
Vrsta i nivo studija: Akademske studije, prvi ciklus			
Naziv predmeta: ZAŠTITA INFORMACIJA			
Nastavnik: Odgovorni nastavnik/saradnik po Odluci Senata			
Status predmeta: Obavezni	Smestar: VI		
Broj ESPB: 7			
Uslov: Nema			

Cilj predmeta:

Sticanje znanja iz oblasti kriptografije: simetrični algoritmi DES,3DES, IDEA, AES i načini rada, asimetrični algoritmi RSA, ECDSA. Upoznavanje sa elementima infrastrukture javnih ključeva PKI (Public Key Infrastructure), digitalnim potpisom i primenama. Izučavanje protokola sigurnosti u računarskim mrežama i na Internetu: TLS, IPSec. Proučavanje zaštite u mobilnim i bežičnim mrežama. Upoznavanje sa primenom i izradom softvera za zaštitu podataka.

Ključne riječi: kriptografija, enkripcija, kriptoanaliza, digitalni potpis, javni ključ, AES, sigurnost u računarskim mrežama.

Sadržaj predmeta

1.	Definisanje osnovnih pojmova iz kriptografije. Model komunikacije i kontrole pristupa.
2.	Klasična(predinformatička) kriptografija
3.	Simetrični moderni kriptografski algoritmi - DES, IDEA
4.	Simetrični moderni kriptografski algoritmi - AES, modovi rada blokovskih algoritama
5.	Simetrični sekvencijalni algoritmi - A5/1, RC4
6.	Kolokvijum 1
7.	Asimetrični algoritmi - RSA
8.	Heš funkcije, digitalni potpisi. Infrastruktura javnog ključa
9.	Protokoli zaštite na aplikativnom sloju. Protokoli kontrole pristupa
10.	Zaštita na transportnom sloju - TLS
11.	Zaštita na mrežnom sloju - IPSec
12.	Kolokvijum 2
13.	Sigurnost mobilnih i bežičnih mreža
14.	Mrežne barijere. Sistemi za detekciju i sprečavanje upada.
15.	Odbrana seminarskih radova.

Literatura:

4. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić Sigurnost računarskih sistema i mreža Mikro knjiga 2007
5. . William Stallings, Osnove bezbednosti mreža, CET, 2014. ISBN: 978-86-7991-376-0
6. Brus Šnajer, Primenjena kriptografija, prevod drugog izdanja, Mikro knjiga

Broj časova aktivne nastave	**Predavanja**: 45	**Vežbe: 45**

Metode izvođenja nastave:

Predavanja, vježbe, obrada studija slučaja (case study), seminarski radovi, prezentacije, kolokvijumi, konsultacije

Ocena znanja (maksimalni broj poena 100)

Predispitne obaveze	Poena 70	Završni ispit	Poena 30
Prisustvo i aktivnost u toku predavanja	**10**	Ispit	**30**
Kolokvijum 1	**30**		
Kolokvijum 2	**30**		