



**Preddiplomski studij
Računarstvo**

Komunikacijske mreže

Pitanja za provjeru znanja
3. blok predavanja

Ak.g. 2007./2008.

Napomena	<p><i>Preporučena literatura, uz bilješke s predavanja, su knjige:</i></p> <ul style="list-style-type: none">• Andrew S. Tanenbaum: <i>Computer Networks, 4th Edition, poglavlje 8 (Network Security)</i>;• Bažant et al.: <i>Osnovne arhitekture mreža, poglavlja 4.6 (Bežični LAN-ovi) i 8 (Pokretljivost u mrežama)</i>
Zadatak 1	<p>Koji se sigurnosni mehanizam koristi za zaštitu od nedozvoljenog korištenja mrežnih resursa:</p> <ul style="list-style-type: none">a) ovjera i ovlašćivanjeb) kriptiranjec) digitalni potpisid) prikrivanje adrese
Zadatak 2	<p>Koji od sljedećih sigurnosnih mehanizama ne pripadaju transportnom sloju:</p> <ul style="list-style-type: none">a) SSLb) TLSc) SOCKSd) IPsec
Zadatak 3	<p>Koja je prednost korištenja virtualnih privatnih mreža?</p> <ul style="list-style-type: none">a) izbjegavanje troškova iznajmljivanja vodovab) slanje prometa s privatne mreže zasebnim vodovimac) pristup anonimnih korisnika korporativnoj mrežid) pristup internetskih korisnika Web poslužitelju korporacije
Zadatak 4	<p>Prevoditelj mrežnih adresa obavlja sljedeću promjenu na IP paketima koji odlaze na Internet</p> <ul style="list-style-type: none">a) mijenja izvorišnu adresub) mijenja odredišnu adresuc) mijenja TTL IP paketad) ne obavlja nikakve promjene na paketu
Zadatak 5	<p>Označite što omogućava primjena sigurnosne stijene:</p> <ul style="list-style-type: none">a) nadzor izlaznog i ulaznog Internet prometab) nadzor prometa koji se razmjenjuje unutar privatne mrežec) ograničavanje broja korisnika privatne mrežed) onemogućavanje zaraze virusom računala unutar privatne mreže

Zadatak 6	Najsigurnija sigurnosna politika u sigurnosnoj stijeni je: a) onemogućiti sav promet pa selektivno dozvoljavati iznimke b) dozvoliti sav promet pa ga selektivno omogućavati iznimke c) samo selektivno omogućavati promet d) samo selektivno onemogućavati promet
Zadatak 7	Koji je način korištenja, od navedenih, karakterističan kod IPsec protokola: a) tunelski način b) jednosmjerni način c) distribuirani način d) agregacijski način
Zadatak 8	Zaglavlje AH služi za a) tuneliranje b) provjeru integriteta c) kriptiranje d) razmjenu ključeva
Zadatak 9	Zaglavlje ESP služi za a) tuneliranje b) kriptiranje c) razmjenu privatnih ključeva d) autentifikaciju
Zadatak 10	Kriptologija je a) znanost o kriptiranju b) umješnost izmišljanja i razbijanja šifri c) znanost o razbijanju šifri d) znanost primjene šifri u umrežavanju
Zadatak 11	Koji od najjači od sljedećih algoritama kriptiranja: a) DES b) AES256 c) 3DES d) Cezarova šifra

Zadatak 12	<p>Problem simetrične kriptografije je:</p> <ul style="list-style-type: none">a) razmjena ključevab) pogađanje ključevac) pronalaženje javnog ključad) generiranje ključae) trajanje kriptiranja
Zadatak 13	<p>Algoritam RSA temelji se na:</p> <ul style="list-style-type: none">a) eliptičkim krivuljamab) složenosti faktORIZACIJEc) neprobojnosti javnog ključad) tajnosti svih ključeva
Zadatak 14	<p>U kakvom su odnosu poruka i njen sažetak:</p> <ul style="list-style-type: none">a) iz poruke nije moguće saznati njen sažetakb) iz sažetka nije moguće saznati porukuc) nikada ne postoje dvije poruke s istim sažetkomd) nikada ne postoji tri ili više poruka s istim sažetkom
Zadatak 15	<p>Modul pretplatničkog identiteta (SIM modul) fizički je smješten:</p> <ul style="list-style-type: none">a) u domaćem lokacijskom registru (HLR)b) u pokretnom komutacijskom centru (MSC)c) u baznoj stanicid) u pokretnoj postaji (MS)
Zadatak 16	<p>Gdje su trajno zapisani svi pretplatnički podaci te trenutna lokacija pretplatnika kod GSM mobilne mreže?</p> <ul style="list-style-type: none">a) VLR (<i>Visiting Location Register</i>)b) MSC (<i>Mobile Switching Center</i>)c) HLR (<i>Home Location Register</i>)d) BSC (<i>Base Station Controller</i>)
Zadatak 17	<p>U GSM mreži, autentifikacijski ključ pretplatnika zapisan je u:</p> <ul style="list-style-type: none">a) u domaćem lokacijskom registru (HLR)b) u pokretnom komutacijskom centru (MSC)c) u baznoj stanicid) u registru identifikacije opreme (EIR)

Zadatak 18	<p>Lokacijsko područje u GSM mreži je:</p> <ul style="list-style-type: none">a) dio domaćeg lokacijskog registra u kojem je pohranjena trenutna lokacija korisnikab) dio domaćeg lokacijskog registra u kojem je pohranjena zadnja poznata lokacija korisnikac) područje pokrivanja radijskim signalom jedne bazne postajed) skup ćelija kroz koje prolazi korisnike) skup ćelija koje pripadaju jednom pokretnom komutacijskom centru
Zadatak 19	<p>Dva načina korisničkog pristupa u digitalnoj mreži integriranih usluga su :</p> <ul style="list-style-type: none">a) temeljni i napredni pristupb) ADSL i ISDN pristupc) osnovni i primarni pristupd) TCP i UDP pristup
Zadatak 20	<p>Karakteristika prve generacije pokretnih mreža (NMT) je:</p> <ul style="list-style-type: none">a) koncept višestrukog pristupa u vremenskoj podjeli (TDMA)b) koncept višestrukog pristupa u kodnoj podjeli (CDMA)c) činjenica da je to analogni sustavd) nepostojanje pristupne mreže, već direktno povezivanje korisnika mreže s jezgrenom mrežom
Zadatak 21	<p>Koji funkcijski entitet se mora dodati komutacijskom čvoru telefonske mreže da bi mogao funkcionirati kao čvor inteligentne mreže?</p> <ul style="list-style-type: none">a) CCAF (<i>Call Control Access Function</i>)b) CCF (<i>Call Control Function</i>)c) SSF (<i>Service Switching Function</i>)d) SDF (<i>Service Data Function</i>)
Zadatak 22	<p>Izbjegavanje sudara okvira u bežičnim LAN-ovima ostvareno je:</p> <ul style="list-style-type: none">a) razmjenom RTS i CTS okvira prije početka razmijene podatakab) uspostavom virtualnog kanala i virtualnog putac) slanjem <i>jamming</i> signala u slučaju nastanka kolizijed) osluškivanjem naponske razine na mediju

Zadatak 23	Dvije osnovne topologije bežičnih lokalnih mreža (WLAN) su: a) infracrveni WLAN i WLAN s radioprijenosom b) infrastrukturni WLAN i neovisni (<i>ad hoc</i>) WLAN c) centralizirani WLAN i decentralizirani WLAN d) privatni WLAN i javni WLAN
Zadatak 24	Kod bežičnih lokalnih mreža (WLAN) susrećemo se s problemom: a) udaljene stanice b) skrivene stanice c) odspojene stanice d) pokretne stanice
Zadatak 25	Primarni pristup (PRA) digitalnoj mreži integriranih usluga (ISDN) u referentnoj točki S sadrži: a) 32 informacijska kanala i 2 signalizacijska kanala b) 2 informacijska kanala i 1 signalizacijski kanal c) 16 informacijskih kanala i 2 signalizacijska kanala d) 1 informacijski kanal i 1 signalizacijski kanal