PREPORUČENA PITANJA ZA PRVI KOLOKVIJUM IZ PREDMETA PRINCIPI MODERNIH TELEKOMUNIKACIJA

1. Koje se osnovne operacije obavljaju u predajniku a koje u prijemniku?
2. Koji su osnovni telekomunikacioni resursi i zašto su oni bitni?
3. Kako se sve mogu klasifikovati signali - po načinu kako su definisani u vremenu, po mogućim vrednostima amplitude i po tome da li imaju slučajnu prirodu.
4. Šta sve može da posluži kao kanal u telekomunikacionom sistemu? Koje se sve pojave mogu javiti u kanalu?
5. Zašto nije zgodno da mobilni telefon radi na učestanostima oko 3MHz? Kolike bi tada bile njegove dimenzije?
6. Model telekomunikacionog sistema sa stanovišta teorije informacija. Opisati pojedine blokove.
7. Kako se definiše količina informacija? Kako se definiše entropija izvora bez memorije? Šta ona predstavlja?
8. Da li prisustvo memorije u izvoru povećava ili smanjuje entropiju? Dati primer izvora s memorijom.
9. Hafmenov kod, efikasnost, stepen kompresije za izvore bez memorije.
10. Koje osobine ima stablo koje odgovara kodu dobijenim Hafmenovim postupkom?
11. Čime je određen maksimalni stepen kompresije diskretnog izvora i kolika je njegova vrednost?
12. Kako se vrše proširenja izvora i koji je njihov značaj? Kako se računa entropija n-tog proširenja izvora?
13. Formulisati prvu Šenonovu teoremu. U čemu je značaj ove teoreme?
14. Lempel-Zivov kod. Poređenje sa Hafmenovim kodom - kada je jedan optimalan a kada drugi?
15. Objasniti način konstrukcije zaštitnog koda sa ponavljanjem. Navesti dva načina odlučivanja pri dekodovanju.
16. U čemu je razlika između detekcije i korekcije? Navesti po jedan kod koji se koristi za ove namene.
17. Formulisati drugu Šenonovu teoremu i objasniti njen značaj.
18. Da li se u digitalnom telekomunikacionom sistemu može obezbediti prenos sa proizvoljnim nivoom pouzdanosti kroz nepouzdan kanal? Ako može, koja je cena koja se za to plaća?
19. Objasniti konstrukciju Hemingovog (7,4) koda. Pojava jednostruke i dvostruke greške.
20. Proširenje koda bitom provere parnosti. Objasniti konstrukciju Hemingovog (8,4) koda i način formiranja sindroma.
21. Objasniti konstrukciju Hemingovog (6,3) koda. Koliko grešaka ovaj kod može da ispravi a koliko da detektuje?
22. Objasniti konstrukciju Hemingovog (16,11) koda. Tumačenje sindroma za razne slučajeve.
23. Šta je kodni količnik zaštitnog koda? Kako povećanje kodnog količnika utiče na informacioni protok (dostupan korisniku) ako je binarni protok u kanalu fiksiran.
24. Jedan izvor emituje niz bita brzinom 1Mb/s i priključen je na kanal u kome je izmerena verovatnoća greške $p=10^{-1}$. Ako se između izvora i kanala umetne optimalan zaštitni koder (a na izlazu kanala optimalan zaštitni dekoder), izračunati za koliko je neophodno povećati binarni protok kroz kanal da bi verovatnoća greške koju registruje korisnik bila zanemarljivo mala.
25. Šta je to interliving i zašto je bitan?
26. Minimalno Hemingovo rastojanje, broj grešaka koji kod može ispraviti i detektovati.
27. Pojam linearnog blok koda, generišuća matrica. Formiranje kodne reči za zadatu informacionu reč.
28. Pojam cikličnog koda, opis generišući polinom. Formiranje kodnog polinoma za zadatu informacionu reč.
29. Sistematski ciklični kod, za šta služi CRC?
30. Nacrtati blok šemu kriptosistema i objasniti osnovne pojmove.
31. Objasniti razliku između tajnosti i autentičnosti.
32. Objasniti šifru transpozicije - kako se konstruiše i kako se može razbiti.
33. Monoalfabetska i polialfabetska šifra.
34. Vernamova šifra, tekući ključ.
35. Princip rada supstitucijskih kutija.
36. Ukratko opisati DES i 3DES algoritam.
37. Ukratko opisati AES algoritam. Koje su četiri osnovne operacije koje se obavljaju u svakoj rundi?
38. Razlika između simetričnih i asimetričnih kriptosistema.
39. Ukratko opisati Difi-Helmanov postupak razmene ključeva.
40. U čemu se ogleda sigurnost RSA algoritma. Zašto je iz javnog ključa teško odrediti tajni ključ?

21.10.2019. Sa Katedre za telekomunikacije