02. 11. 2019.

Prvi kolokvijum

PRINCIPI MODERNIH TELEKOMUNIKACIJA

P1. a) Kako se definiše količina informacija? Kako se definiše entropija izvora bez memorije i šta ona predstavlja? (5p)

b) Čime je određen maksimalni stepen kompresije binarnog diskretnog izvora i kako se on može izračunati? (5p)

P2. a) Opisati monoalfabetsku i polialfabetsku šifru. Šta je to Vernamova šifra? (3p)

b) Objasniti razliku između simetričnih i asimetričnih kriptosistema. (3p)

c) Opisati ukratko RSA algoritam. Zašto je iz javnog ključa teško odrediti tajni? (4p)

Z1. Izvršiti Hafmenovo kodovanje izvora informacija bez memorije koji emituje pet simbola sa verovatnoćama datim u tabeli:

s_i	s_1	s_2	s_3	s_4	s_5
$P(s_i)$	0,0625	0,5	0,125	0,0625	0,25

a) Odrediti entropiju izvora a zatim efikasnost i stepen kompresije dobijenog koda. Nacrtati kodno stablo koje odgovara Hafmenovom kodu. (3p)

b) Ako se na izlaz Hafmenovog kodera priključi zaštitni koder sa ponavljanjem tri puta a zatim kanal u kome je verovatnoća greške $p=10^{-2}$, odrediti ukupan broj binarnih simbola koji se šalju kroz kanal ako izvor emituje 1000 simbola. Koliku verovatnoću greške tada registruje korisnik (pravilo odlučivanja u dekoderu izaberite sami, kako god želite)? (4p)

c) Ako je primenjen optimalni nedestruktivni statistički kod i optimalan zaštitni kod, koliki je minimalan broj binarnih simbola koji treba poslati kroz kanal ako izvor emituje 1000 simbola i ako kanal unosi greške nasumično sa verovatnoćom $p=10^{-2}$, ako se zahteva da verovatnoća greške koju registruje korisnik bude zanemarljivo mala. (3p)

Z2.

a) Niz informacionih bita 100001 kodovati Hemingovim (6,3) kodom. Kao posledica grešaka koje se javljaju u kanalu 2, 7. i 8. bit u poslatoj sekvenci nisu ispravno primljeni. Kakvi zaključci se mogu doneti nakon procesa dekodovanja? (6p)

b) Ako se greške u kanalu pojavljuju sa verovatnoćom $p=10^{-4}$ i ako je primenjen kod iz prethodnog dela zadatka, izračunati verovatnoću da se u kodnoj reči pojavi dvostruka greška. (2p)

c) Na koji način se može napraviti Hemingov kod (7,3), koji ima sposobnost da detektuje dvostruke greške? (2p)