

LUCRAREA DE CASĂ nr.2
pentru anul II electronică, grupa 10703

- Problemele care urmează sunt în bună parte personalizate: parametrul k (cu semnificația poziției în catalogul grupei conform tabelului atașat la finalul acestor pagini) face unele enunțuri particulare.
- Se cer soluții concise, numerice (precizia: patru cifre zecimale după virgulă), însoțite de comentarii la obiect atunci când este necesar.
- Soluțiile sunt punctate. Punctele acumulate din soluții corecte și complete trebuie confirmate printr-o susținerea orală competentă în ziua examenului. Pentru notă de promovare sunt necesare cel puțin **60** de puncte. Nota maximă se acordă pentru **120** de puncte. Notele intermediare se acordă prin interpolare liniară între aceste limite, în raport cu punctajul efectiv realizat.
- Soluțiile trebuie redactate pe mijloace electronice, cu un editor de texte din cele cunoscute și trebuie prezentate în formă tipărită până în **22 aprilie 2016**. Orice depășire a termenului precum și folosirea altui k , diferit de cel alocat individual echivalează cu lipsa lucrării și se notează cu nota 1 (unu).

ENUNȚURI

Problema 1. Canal, informație mutuală, capacitate

Se dă un canal caracterizat de matricea $P = \begin{bmatrix} p_1 & 1 - p_1 \\ 1 - p_2 & p_2 \end{bmatrix}$, cu

$$p_1 = 0,75 + 0,02 \cdot (k/30)$$

$$p_2 = 0,77 + 0,02 \cdot (k/30)$$

- a. Care este transinformația (informația mutuală) când la intrarea canalului debitează o sursă fără memorie cu probabilitatea primului simbol dată de expresia $p = 0,2 + 0,2 \cdot (k/30)$? (10 puncte)
- b. Care este capacitatea canalului? (10 puncte)
- c. Faceți canalul să fie simetric și repetați calculele de la punctele anterioare. Comparăție. (15 puncte)

Problema 2. Coduri compacte

Utilizați din nou sursa de informație de la **Problema 1**. Construiți extensia ei de ordinul 3.

- a. Stabiliți un cod binar compact pentru această sursă extinsă. (10 puncte)
- b. Calculați lungimea medie a codului stabilit. (10 puncte)
- c. Comparați entropia sursei cu lungimea medie a codului. (5 puncte)

Problema 3. Codarea aritmetică

Luați numele de familie propriu, așa cum îl găsiți în tabelul de la sfârșitul acestor pagini și ignorați semnele diacritice.

Frecvențele simbolurilor alfabetice se admit a fi cele din tabelul alăturat.

Simbol	A	B	C	D	E	F	G	H	I	J	K	L	M
Frecvența	10	2	5	4	9	2	2	1	10	1	1	5	3

Simbol	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frecvența	6	5	4	1	6	6	6	5	2	1	1	1	1

Scrieți un cod aritmetic al numelui propriu. (20 puncte)

Problema 4. Compresia de date LZW

Se consideră șirul de caractere *abracadabra*.

- Compuneți dicționarul folosit la comprimarea/decomprimarea acestui șir prin algoritmul Lempel-Ziv-Welch (LZW). (10 puncte)
- Scrieți explicit secvența de coduri numerice asociată șirului dat. (10 puncte)

Problema 5. Criptarea cu cheie publică

Se dă perechea de numere prime $(p, q) = (929, 997)$. Perechea (p, q) se utilizează într-un sistem de criptare cu cheie publică de tipul Rivest-Shamir-Adleman (RSA). Cheia făcută cunoscută public este de forma $[5, n]$ cu $n = p \cdot q$.

- Calculați cheia privată. (10 puncte)
- Numărul $m = 10703 \cdot k$ este considerat a fi *textul clar*. Care este rezultatul criptării (*textul cifrat*)? (10 puncte)
- Se consideră acum că *textul cifrat* privit ca număr este mai mare cu o unitate decât cel calculat la punctul b. Care este în acest caz rezultatul decriptării? (15 puncte)

<i>k</i>	Grupa 10703		<i>k</i>	Grupa 10703
1	Anghelache		16	Marinescu Nicoleta
2	Boboc		17	Mihai Daniel
3	Burada		18	Mihai Ionuț
4	Călin		19	Mocanu
5	David		20	Paraschiv
6	Dobre		21	Podăreanu
7	Drăghici		22	Șerban Andrei
8	Dugăiașu		23	Șerban Dumitru
9	Dumitru		24	Sima
10	Fulgeanu		25	Simion
11	Ionescu George		26	Sârbu
12	Ionescu Robert		27	Stanciu
13	Ivan		28	Virgilio Milton Gomes
14	Lupu		29	Vlăsceanu
15	Marinescu Marian		30	Zamfir