SzA XIV. gyakorlat

2008. december 10/11.

Hasznos tudnivalók

- RSA: p, q prímek (választjuk), $n = pq$, $m = \varphi(n) = (p-1)(q-1)$, $1 \leq e \leq n$ úgy, hogy $(e, m) = 1$ (választjuk), d-hez megoldjuk $ed \equiv 1 \mod m$-et. Nyilvános kulcs: (n, e), titkos kulcs: (n, d). Kódolófüggvény: $f(X) = X^e \mod n$, dekódolófüggvény: $f^{-1}(Y) = Y^d \mod n$.

Feladatok

1. Írjuk fel $\pi \circ \rho$-t, ciklikus módon, ha

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 8 & 4 & 2 & 7 & 6 & 3 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 8 & 7 & 4 & 6 & 3 \end{pmatrix}$$

2. Az S_7 szimmetrikus csoport egy eleme az (12)(356) permutáció. Mi ennek az elemnek a rendje?

3. Határozzuk meg az (12)(345)(6789) permutáció inverzét!

4. Mik a D_6 diédercsoport elemei? Mik az elemek rendjei? Ciklikus-e ez a csoport? Adjuk meg D_6 egy ciklikus részcsoportját!

5. Elfogtunk egy Katona tanár úrtól Fleiner tanár úrhoz tartó e-mailt, amelynek tárgya: `Re: Milyen anyagot kell tudni a pótpótzh-ra?` Sajnos a tartalom RSA-val titkosítva van Fleiner tanár úr nyilvános kulcsával, ami $(85, 43)$. Ezeket a számokat látjuk az üzenetben: 47, 46, 6, 8, 3, 8, 38, 58, 27, 66, 72, 3, 58, 27, 8, 27, 67, 48, 3, 56, 48, 76, 67, 48, 27, 56, 48, 27, 81, 12, 7, 7, 8, 3. Mi az eredeti szöveg, ha a karakterkódolás az alábbi táblázat szerint történik?

A	2	B	3	C	4	D	6	E	7	F	8	G	11	H	12	I	13
J	21	K	22	L	23	M	26	N	27	O	28	P	31	Q	32	R	33
S	36	T	37	U	38	V	41	W	42	X	43	Y	46	Z	47		48

6. Kérdések feltevése az anyag nem értett részeivel kapcsolatban a gyakvezérnek.

7. Tanulás. Megértés.

8. Jól sikerült vizsga.

9. Öröm.

Ez volt az utolsó gyakorlat, vége a félévnek, kéremkapcsojjaki!