

KÓDOLÁSTECHNIKA GYAK_IV

2007. január 11.

1. Egy lineáris bináris blokk kód paritásellenőrző mátrixa $H=[11111]$. Adja meg a kód

- a.) szisztematikus generátormátrixát! (5p)
- b.) Tud-e törléses hibát javítani a kód? (5p)

2. Tekintsük a $0 \rightarrow 000000$, $1 \rightarrow 111111$ hibajavító kódolást.

- a.) perfekt-e a kód? (5 p)
- b.) adja meg a dekódolás hibavalószínűség formulát emlékezetnélküli BSC(p) csatorna esetén (5p)

3. $g(x)=x^8+x^2+1$ polinommal CRC-t generálunk. Adja meg a CRC-t, ha a védendő adatblokk 0000 0000 0000 0111. (10p)

4. RSA kódoló algoritmus esetén a kulcsok előállításához $p=7$, $q=17$ prímekből indultunk ki.

- a.) Adja meg a lehető legkisebb kódoló kulcsként használható exponenst! (3p)
- b.) Számítsa ki az $x=11$ nyílt szöveghez tartozó y rejtett szöveget! (3p)
- c.) Határozza meg a dekódoló kulcsot! (4p)

5. Adja meg a 36 darab a betűből álló karaktersorozat LZ78-kódját! (10p)

6. Tömören, formálisan fejtse ki:

- a.) kétdimenziós paritáskód (kód paraméterei, kódolás algoritmus) (5 p)
- b.) egyirányú hash függvény, ütközésellenálló hash függvény (5 p)
- c.) Max-Lloyd algoritmus (10 p)

Pontozás: 1: <=24 2:25- 34 3: 35 - 45 4: 45- 54 5: 55– 70

KÓDOLÁSTECHNIKA GYAK_IV MEGOLDÁSOK

2007. január 11.

1. a.) $G = \begin{pmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{pmatrix}$ b.) igen, $d=2, t=d-1=1$

2. a.) perfekt nem perfekt formula (a konkrét adatokkal is):
 $2(1+6+15) < 64$

3.) $x^{10} + x^9 + x^8 \pmod{g(x)}$ maradékot kell meghatározni. Így a keresett 8 bites CRC:
00011011.

4.) RSA műveletek eredményei

a.) $e=5$ b.) $y=44$ c.) $c=77$

5.)

Az LZ78-kódolás egyes lépéseit bejelöltük a bemeneten:

a|aa|aaa|aaaa|aaaaa|aaaaaa|aaaaaaa|aaaaaaaa

kódoló szótár

kimenete	index	bejegyzés
$\langle 0; f(a) \rangle$	1	a
$\langle 1; f(a) \rangle$	2	aa
$\langle 2; f(a) \rangle$	3	aaa
$\langle 3; f(a) \rangle$	4	$aaaa$
$\langle 4; f(a) \rangle$	5	$aaaaa$
$\langle 5; f(a) \rangle$	6	$aaaaaa$
$\langle 6; f(a) \rangle$	7	$aaaaaaa$
$\langle 7; f(a) \rangle$	8	$aaaaaaaa$
$\langle 8; f(a) \rangle$	9	$aaaaaaaaa$

6.

a.) adatbitek $k_1 \times k_2$ méretű mátrixba rendezése, soronként oszloponként paritásbit számítása
paraméterek $C(n=(k_1+1)(k_2+1), k=k_1k_2, d=4)$

b.)

nehéz feladat adott hash értékre vezető inputot találni (egyirányúság)

nehéz feladat adott hash értékre vezető (ütköző) két különböző inputot találni (ütközésmentesség)

c.) *A Lloyd–Max-algoritmus:*

A kvantálót egyértelműen jellemzik az x_i kvantálási szintek és a $B_i = (y_{i-1}, y_i]$ tartományok. Célunk a szintek és az intervallumhatárok javítása lépésről lépésre.

1. Vegyünk fel egy közelítést a kvantálási szintekre.

2. Optimalizáljuk a kvantálót a kvantálási szintek szerint, vagyis határozzuk meg az intervallumhatárokat a legközelebbi szomszéd feltétel kielégítésével.

3. Számítsuk ki, hogy mennyivel csökkent a torzítás, és ha ez egy előre meghatározott küszöbértéknél kisebb, akkor készen vagyunk.

4. Optimalizáljuk a kvantálót az imént kapott intervallumokhoz, vagyis alkalmazzuk a súlypont feltételt, és folytassuk az algoritmust a 2. ponttól.