

Név/Kód:

--	--	--	--	--	--	--	--

F
O
N
T
O
S
!!!

1. (10p)	2. (20 p)	3. (20 p)	4. (20 p)	5. (30 p)	Összesen (100p)	Jegy
----------	-----------	-----------	-----------	-----------	--------------------	------

F
O
N
T
O
S
!!!

- Minden feladatot külön lapon dolgozzon ki és minden lapon olvashatóan szerepeljen a neve és a NEPTUN kódja!
- A diákigazolványa legyen előkészítve!
- A példák megoldása során, az előadáson elhangzott konvenciókat alkalmazza!
- A FELADATOK MEGOLDÁSA MELLÉ INDOKLÁST IS KÉRÜNK! ÖNMAGÁBAN CSAK A HELYES VÉGEREDMÉNY NEM ÉRTÉKELHETŐ.

A fentiek nem teljesítése esetén a dolgozata nem értékelhető!!!

1. Karikázza be a helyes válaszokat (a pontszám csak akkor kapható meg, ha az összes helyes választ megadta)!
- Ha egy kód l hosszúságú bursthibát képes javítani, akkor a kódszavak bursthosszúsága nagyobb mint $2l$.
 - A $C(n,k)$ paraméterű ciklikus kódoknál a paritásellenőrző polinom fokszáma k .
 - Egy szindrómavekört a generátormátrixszal szorozva megkapjuk a hibavektort.

d) Az RS kód hibajavító képessége $t = \left\lfloor \frac{n-k}{2} \right\rfloor$

2. m darab véletlen blokkból álló üzenetünket rejtjelezve és integritásvédelemmel szeretnénk továbbítani. Integritásvédelemül azt a gyors módszert választjuk, hogy az m darab üzenetblokkot mod 2 összegezzük, s így egy ellenőrző összeg blokkot nyerünk (azaz az ellenőrző összeg blokk i -edik bitje az üzenetblokkok i -edik bitjeinek a mod 2 összege). Ezután az $m+1$ darab blokkot blokkonként ECB módban rejtjelezzük.
- Lehallgató támadó sikeres lehet-e? (6p)
 - Ha megengedjük a kimerítő kulcskeresés elméleti lehetőségét is, meg tudnánk-e fejteni a nyílt szöveget? Hogyan? (8p)
 - Integritásvédelemre alkalmas-e a módszer? (6p)

3. Adott a következő kódtábla és forráseloszlás

Forrásszimbólumok	Valószínűségek	Kódszavak
X1	0.4	0
X2	0.2	10
X3	0.2	110
X4	0.2	1111

- Menni az átlagos kódszóhossz? (5p)
- Milyen távol van a kód a tömöríthetőség elvi alsó korlátjától? (5p)
- Prefix-mentes-e a kód? (5p)
- Optimális-e a kód? (5p)

- 4 Tömörítse a 010001010010100011 sorozatot a szótáralapú Lempel- Ziv algoritmussal

- 5 Adja meg a $C(7,5)$ RS kód generátorpolinomját. (10p)

Jelzeze hány hibát képes javítani a kód. (10p)

Adja meg azon kódszóvektor komponenseit GF(8) feletti szimbólumokkal, ami az $\mathbf{u} = (7, 7, 7, 7, 7)$ üzenetvektorhoz tartozik (10p).

(Konvencióként a vektor és polinomok közötti kapcsolatnál a balról kezdődő komponenshez a legnagyobb fokszám tartozik pl. $(2, 3, 4) \rightarrow 2x^2 + 3x + 4$) A hatványtábla: $y^0 \rightarrow 1; y \rightarrow y; y^2 \rightarrow y^2; y^3 \rightarrow y + 1; y^4 \rightarrow y^2 + y; y^5 \rightarrow y^2 + y + 1; y^6 \rightarrow y^2 + 1; y^7 \rightarrow 1$

Elégtelen	Elégséges	Közepes	Jó	Jeles
0-39 pont	40-53 pont	54-67 pont	68-81 pont	82-100 pont