

Kódok

Összeállította Hraskó András és Szőnyi Tamás

Bevezetés

Az adatok továbbításának három fő problémája a *biztonság*, a *titkosság* és a *tömörség*. A biztonság kérdésének matematikai alapjaival a *kódelmélet*, a titkosságéval a *kriptográfia*, a tömörséggel elsősorban az *információelmélet* foglalkozik, de ez a három témakör nem különíthető el ennyire mereven.

A kriptográfia témakörében a **[Singh]**, az információelmélettel kapcsolatban az **[info]**, **[kom]**, **[bev]** könyveket ajánljuk az érdeklődőknek. Ebben a cikkben a biztonság kérdését, a kódelmélet alapkérdéseit vizsgáljuk. Néhány, a témával kapcsolatos szituáció a gyakorlatban:

1. Azonosítók

Az állampolgárokat, a könyveket, a bolti árukat, a vasúti kocsikat stb. mind nyilvántartják valahol, és ehhez azonosítókat használnak.

Az állampolgárok esetében ez (volt korábban) a személyi szám, a könyveknél az ISBN szám (International Standard Book Number), az áruk esetében az EAN szám (European Article Numbering system). Az azonosítókat emberek "viszik be" a rendszerbe, illetve az azonosítók alapján emberek kérdeznak le információkat. Az ember többször hibázik, mint a számítógép. Hajlamosak vagyunk a begépeléskor elütni egy-egy karektert, néha pedig fölscerélünk kettőt. Az ilyen hibák nem okoznak túl nagy galibát, amikor egy amúgy értelmes szöveget olvasunk, de súlyos kellemetlenségek forrásai lehetnek egy adatnyilvántartó rendszerben. Ezért a nyilvántartási számokat úgy alakítják ki, hogy ilyen hibák lehetőleg ne fordulhassanak elő.

2. Sérülékeny adattárak és kommunikációs csatornák

Egy lassan már mindenki által ismert információ hordozó a CD (Compact Disc). Kedvenc zenelemezőnként gyakran vesszük kézbe, könnyen előfordulhat, hogy ujjunkról zsírfolt kerül rá, por tapad meg rajta, az se kizárt, hogy megkarcoljuk. A fölvétel során olyan kódolási eljárást alkalmaznak, hogy a lemez lejátszása során, a dekódoló berendezés az ilyen hibákat nagymértékben fel tudja ismerni, sőt ki tudja javítani és a hibák ellenére az eredeti felvételt játssza le.

A Mariner és Voyager szondák képeket küldtek Naprendszerünk bolygóiról a Földre. Ezek a nagyon távolról jött jelek hihetetlenül gyengék, így a vevőberendezésben óhatatlanul meglevő zaj miatt könnyen félreérthetőek. Ha nem használtak volna kódolási eljárást, akkor a fényképek teljesen használhatatlanok lennének.

Feladatokon, azok megoldásain és a CD matematikájáról írt rövid esszé segítségével szeretnénk tanároknak és diákoknak bevezetést adni a kódolás témakörébe. A feladatgyűjteményben tematikusan gyűjtöttük össze a feladatokat. Órán, szakkörön más sorrendben érdemes haladni. Az alábbi fileokban úgy található meg a téma kidolgozása, ahogy az Hraskó Andrásnak a 2002-2003. tanévben a 11-12-es diákoknak meghirdetett tehetséggondozó szakkörön sikerült: 1. szakkör (zip), 2. szakkör (zip), 3. szakkör (zip), 4. szakkör (zip), 5. szakkör (zip), 6. szakkör (zip), 7. szakkör (zip).