Stærðfræðimynstur í tölvunarfræði

Vikublað 7

Í þessari viku ljúkum við umfjöllun um talnafræði með því að fara í RSA dulkóðunaraðferðina á bls. 191-194 í kafla 2.6. Síðan förum við aftur í sannanir og skoðum kafla 3.1 og 3.3.

Í næstu viku verður farið í talningafræði í kafla 4

Hér að neðan eru 5 skiladæmi sem þið eigið að skila í hólf dæmatímakennara ykkar fyrir hádegi mánudaginn 17. október. **Munið að merkja skilin ykkar með númeri dæmahóps og nafni dæmatímakennara.** Auk þess eru nokkur dæmi í viðbót sem þið ættuð að nota til að æfa ykkur og fullvissa ykkur um að þið skiljið efni. Farið verður í einhver af þeim í dæmatímunum eftir því sem tími vinnst til.

Skiladæmi 7

1. Strengurinn "QSJUVCHA" hefur verið kóðaður með Sesars kóðun (e. Caesar cipher) (sjá bls. 165). Þið eigið að afkóða strenginn þó þið vitið ekki dulmálslykilinn. Lykilinn er tala frá 1 til 25, sem táknar hliðrun bókstafanna í enska stafrófinu. Þið munuð þekkja afkóðaða strenginn þegar þið sjáið hann.

2. Í þessu dæmi eigið þið að nota RSA dulkóðunaraðferðina til að kóða og afkóða. Eins og gert er í bókinni þá notum við lykilinn $n = 43*59$ og $e = 13$. Aðeins eru notaðir enskir hástafir og þeir kóðaðir með gildunum 0 til 25 (þ.e. A er 0, B er 1, o.s.frv.). Það er nauðsynlegt fyrir ykkur að nota eitthvert táknreikniforrit til að leysa þessi verkefni, t.d. ARIBAS.
    a. Dulkóðið orðið "BAUGUR" með RSA aðferðinni. Takið tvo og tvo stafi saman og skilið þremur heiltölum.
    b. Afkóðið skeytið 2299 0468 yfir í bókstafi með RSA aðferðinni. Þetta verður fjögurra stafa orð sem þið eigið að þekkja.

3. Dæmi 2 í kafla 3.1 á bls. 223 í kennslubók.
   [Þýðing: Sannið að ef n er jákvæð oddatölu heiltala þá gildir að $n^2 \equiv 1 \pmod 8$.]

4. Dæmi 20 í kafla 3.1 á bls. 224 í kennslubók.
   [Þýðing: Sannið að annað veldið af tölu sem ekki er deilanleg með 5 hefur afganginn 1 eða 4 þegar deilt er í hana með 5. (*Vísbending:* Notið sönnun með því að skoða öll tilfelli.]

5. Dæmi 8 í kafla 3.3 á bls. 253 í kennslubók.
   [Þýðing: Sýnið að $1^3 + 2^3 + ... + n^3 = [n(n + 1)/2]^2$ þegar n er jákvæð heiltala.]

Skilið þessum dæmum fyrir hádegi mánudaginn 17. október.

Að auki skuluð þið líta á eftirfarandi dæmi:

Úr kafla 2.6:
    45, 47.
Úr kafla 3.1:
    3, 7, **23**, 27, **49**.
Úr kafla 3.3:
    7, **13**, 17, 21, 25, 39, 73.

Munið að dæmin að ofan eru æfingadæmi og að þið græðið mest á því að reyna að leysa þau sjálf (en ekki að horfa á einhvern annan leysa þau!). Feitletruðu dæmin eru "athyglisverðari" en hin og líklegra að farið verði í þau í dæmatímunum.

---

hh (hja) hi.is, 10. október, 2005.