Stærðfræðimynstur í tölvunarfræði

Vikublað 9

Í þessari viku verður lokið umfjöllun um Þríhyrning Pascal úr kafla 4.4. Síðan verður farið stuttlega í líkindafræði í kafla 5.1, en þar á eftir verður byrjað á venslum (e. relations) í kafla 7. Kafla 6 er öllum sleppt.

Í næstu viku verður haldið áfram með venslin.

Í þessari viku þurfið þið ekki að glíma við skiladæmi, heldur getið þið spreytt ykkur á áhugaverðum verkefnum. Þið þurfið ekki að skila þessum verkefnum, en við munum fara yfir þau verkefni sem koma inn og velja 3-4 best leystu verkefnin. Þeir nemendur sem eiga þau verkefni fá í verðlaun einkunnina 10 fyrir öll eldri heimadæmi (þ.e. heimadæmi 1 til 8).

Hér að neðan eru verkefnin. Veljið eitt af þeim til að gera og setjið lausn ykkar fram á þann hátt að hægt sé að setja lausnina á heimasíðu námskeiðsins ef hún verður fyrir valinu sem ein af áhugaverðustu lausnunum. Þið getið til dæmis sett lausnina fram sem Word skjal eða sem gagnvirka Vefsíðu.

Linuleg samleifaraðferð

Eins og þið munið þá er línulega samleifaraðferðin (e. linear congruential method, LCM) ein af þeim aðferðum sem notaðar eru til að búa til gervislembitölur. Aðferðin notar formúluna $x_{n+1} = (ax_n + c) \bmod m$. Ekki öll gildi á a, c og m gefa aðferð með full lotu (þ.e. öll gildi frá 0 til m-1 koma fyrir sem slembitölur). Skoðið þetta val á stikunum a, c og m og hugið sérstaklega að eftirfarandi atriðum:

- Ef búa ætti til slembitölugjafa sem gæfi 8 bita slembitölur, er hægt að finna gildi á a og c sem gefur fulla lotu ef við festum m sem 256? Hvað með 16 bita slembitölur (þ.e. $m = 65536$)?
- Skoðið slembitölugjafann í Java (þ.e. `Random` klasann) og fullvissið ykkur um að hann gefi fulla lotu.
- Hvað með *slembni* (e. randomness) slembitölugjafans? Eru mismunandi gildi á a, c og m sem gefa mismunandi slembna gjafa?

RSA afkóðun

Ósamhverfa dulkóðunaraðferðin RSA byggir á því að erfitt sé að þátta tölur. Hér fáið þið gefinn almenningslykil (n, e) ásamt skilaboðum sem hafa verið kóðuð með honum. Þið eigið að finna upphaflegu skilaboðin með því að finna fyrst einkalykilinn (n, d) út frá almenningslyklinum og nota hann til að afkóða skilaboðin.
Lykilinn sem þið fáið er
(221873272483254945141922353186910788703120217007463592538956281140602541064561, 65537). Hér er n 257-bita tala og e er 65537. Hér er n á sextándakerfisformi: (01 EA87 D26D AE2B B5E4 DC33 6EE0 D994 DB82 FE49 F895 5D80 0E36 6B76 722C 1016 4171) $_{16}$. Þar sem n er 257-bita (þ.e. rúmlega 32 bæti) þá er hægt að kóda 32 bókstafi í einni tölu, sem er lægri en n, ef við skeytum saman ASCII-kódum stafanna. Skeytið sem þið eigið að reyna að finna er kóðað í tveimur 257-bita tölum. Það er því á bilinu 33 til 64 stafir að lengd. Tölurnar eru

- 10428173539199542612778090092764752941275400416049065681174903099165334589931 1
  eða (00 E68D 5EDF 3416 FF31 D5FC 22D5 2E24 26DC 5141 8733 85D4 18C7 AA7E 1368 3D23 332F) $_{16}$
- 17133725640724979429389717560992499472298950593896069663884858854963770730541 9
  eða (01 7ACD 7355 13A8 5617 B44C 69EA 00DD 8870 54C4 08AF 6E02 CEDA 268E D44E 7E3A 91CB)$_{16}$

Til þess að þið vitið hvort þið séuð á réttri leið þá hefst skeytið svona: "Nú ...". Fyrstu þrír stafirnir eru því 'N' (78), 'ú' (250) og ' ' (32). Skilið lýsingu á aðferðinni sem þið notuðuð til þess að brjóta upp aðferðina, ásamt lausninni að sjálfsögðu.

Athugið að nú eru yfirleitt notaðir 1024-bita lyklar (þ.e. stærðin á n) í RSA, en þeir sem vilja meira öryggi nota 2048-bita lykla. Ykkur ætti því ekki að vera skotaskuld úr því að brjóta upp 257-bita lykil!

Hip

Leikurinn Hip er spilaður á NxN borði þar sem N er oddatala. Í upphafi er borðið tómt, en leikmenn skiptast á að leggja niður steina, annar hefur hvíta steina, hinn svarta. Markmiðið í leiknum er að komast hjá því að láta 4 steina af sama lit mynda fern á borðinu. Fernur þarf ekki endilega að vera samsíða hliðum borðsins. Hann gæti verið halla (sjá myndir af fernum). Þið eigið að greina leikinn og skrifa skýrslu um það sem þið komist að.

- Reiknið út fjölda mögulegra fernra sem eru á NxN borði.
- Skoðið tilfellin N=5 og N=7. Er til áætlun fyrir annan leikmanninn sem tryggir honum sigur?
- Hversu marga mögulega leiki er um að ræða (t.d. fyrir N=5 og N=7)?

- Hvernig lítur leikjatré (e. game tree) (sjá bls. 651-656 í kennslubók) þessa leikjar út (skoðið fyrstu lögin)?

Skilafrestur á verkefnunum er til **hádegis mánudaginn 31. október** og það á að skila þeim beint til mín. Þið ráðið hvort þið skilið verkefnunum í tölvupósti eða í hólfið í VR-II.

Í dæmatímum í næstu viku (1.-2. nóv.) eigið þið að reyna að leysa valin dæmi úr efni námskeiðsins hingað til. Dæmatímakennararnir munu ganga á milli og aðstoða, en munu ekki vera með kennslu að öðru leyti. Þið *þurfið* ekki að mæta í þessa tíma, en það er mikilvægt fyrir þá sem hafa misst af einhverju efni, eða vilja sjá hvernig þeir standa að nýta sér þetta tækifæri.

Dæmin sem leysa á í dæmatímunum í næstu viku verða tilkynnt síðar.

---

hh (hja) hi.is, 24. október, 2005.