1. Homne kuupäev

1 sekund 20 punkti

Kirjutada programm, mis leiab antud kuupäevale Gregoriuse kalendris järgneva kuupäeva.

Sisend. Tekstifaili `homme.sis` ainsal real on antud kuupäev kujul $PP.KK.AAAA$ (tegu on kalendris eksisteeriva kuupäevaga, kus $1000 \leqslant AAAA \leqslant 9000$).

Väljund. Tekstifaili `homme.val` ainsale reale väljastada sisendis antud kuupäevale järgnev kuupäev samal kujul.

Näide.

`homme.sis`	`homme.val`
`01.01.2004`	`02.01.2004`

Näide.

`homme.sis`	`homme.val`
`31.12.2004`	`01.01.2005`

Märkus. Liigaastad on need, mille number jagub neljaga, välja arvatud need, mille number jagub sajaga (need on lihtaastad), välja arvatud need, mille number jagub neljasajaga (need on jälle liigaastad).

Märkus. Ülesanne tuleb lahendada arvuti süsteemset kuupäeva muutmata. Seda nõuet eiravad lahendused diskvalifitseeritakse.

2. Ratsukäik

1 sekund 40 punkti

Antud malelaua kahe välja koordinaadid. Kirjutada programm, mis leiab maleratsu minimaalse käikude arvuga teekonna esimeselt väljalt teisele.

Sisend. Tekstifaili `ratsu.sis` esimesel real on lähtevälja koordinaadid kujul VR, kus V on veerutähis $a \ldots h$ ja R on reatähis $1 \ldots 8$. Faili teisel real on sihtvälja koordinaadid samal kujul.

Väljund. Tekstifaili `ratsu.val` esimesele reale väljastada minimaalne lähteväljalt sihtväljale liikumiseks kuluvate käikude arv K. Järgmisele $K+1$ reale väljastada ratsu teekond lähteväljalt alates. Kui minimaalse pikkusega teekondi on mitu, väljastada ükskõik milline neist.

Näide.

`ratsu.sis`	`ratsu.val`
`a1`	`3`
`b1`	`a1`
	`c2`
	`a3`
	`b1`

Märkus. Maleratsu võib ühe käiguga liikuda kas kaks sammu (kahe välja võrra) horisontaalis ja ühe sammu vertikaalis või ühe sammu horisontaalis ja kaks sammu vertikaalis.

Hindamine. Selles ülesandes saavad 50% punktidest lahendused, mis leiavad õigesti vajalike käikude arvu, kuid ei leia käike endid.

3. XOR-šifreerimine

avatud testid 40 punkti

Tehe "välistav või" (ehk XOR, mida tähistatakse ka $\oplus$) on loogiline tehe kahe tõeväärtuse vahel, mille tulemus on "tõene", kui täpselt üks operandidest on "tõene", ja "väär" igal muul juhul.

Kahe kahendarvu "liitmisel" $\oplus$-tehte abil tõlgendatakse operandide iga bitti tõeväärtusena (1 = "tõene", 0 = "väär"), rakendatakse $\oplus$-tehet kummagi operandi vastavatele bittidele (ühelised omavahel, kahelised omavahel jne) ning koostatakse saadud tulemustest uus kahendarv.

Näiteks $0101_2 \oplus 1100_2$ arvutatakse järgmiselt: ühelised $1 \oplus 0 = 1$; kahelised $0 \oplus 0 = 0$; neljalised $1 \oplus 1 = 0$; kaheksalised $0 \oplus 1 = 1$. Kokku saame seega $0101_2 \oplus 1100_2 = 1001_2$. Kuna kahe biti $\oplus$-summa on alati üks bitt, siis ülekandeid $\oplus$-liitmisel ei ole.

Vaatleme klassikalist $\oplus$-liitmisel põhinevat algoritmi andmete salastamiseks ehk šifreerimiseks: l-bitise kahendarvu t šifreerimiseks kasutame l-bitist võtit k ja salatekstina ehk krüptogrammina edastame summa $s = t \oplus k$. Summa s ja võtme k valdaja saab esialgse teate hõlpsasti taastada ehk dešifreerida, arvutades $t = s \oplus k$. See toimib, sest $\oplus$ on iseenda pöördtehe: mistahes t ja k korral $s \oplus k = t \oplus k \oplus k = t$.

Nüüd on juhtunud nii, et üht teksti T šifreeriti mitme erineva võtmega ja pärast seda läks teksti originaal kaduma. Alles on kõik N kasutatud šifreerimisvõtit K_1, K_2, ..., K_N, samuti kõik N krüptogrammi E_1, E_2, ..., E_N, kuid pole teada, milline krüptogramm on saadud millise võtmega. Vaja on säilinud andmete põhjal taastada esialgne tekst T.

Sisend. Tekstifaili `xor.sis` esimesel real on tühikuga eraldatud täisarvud N ja L. Järgmisel N real on igaühel L tühikutega eraldatud 8-kohalist kahendarvu: teksti T šifreerimiseks kasutatud võtmed $K_{1...N}$. Järgmisel N real on samuti igaühel L tühikutega eraldatud 8-kohalist kahendarvu: saadud krüptogrammid $E_{1...N}$ mingis juhuslikus järjekorras.

Väljund. Tekstifaili `xor.val` ainsale reale väljastada L tühikutega eraldatud 8-kohalist kahendarvu: üks võimalik tekst T. Kõik arvud väljastada täpselt 8-kohalistena (võivad alata nullidega).

Näide.

`xor.sis`
```
3 3
01010101 01010101 01010101
10101010 10101010 10101010
11111111 11111111 11111111
10111010 10110110 10110000
00010000 00011100 00011010
11101111 11100011 11100101
```

`xor.val`
```
01000101 01001001 01001111
```

Vastuse õigsuse kontroll: $T = 01000101_2 01001001_2 01001111_2$ šifreerimisel ...

- ... võtmega $K_1 = 01010101_2 01010101_2 01010101_2$
  saame küptogrami $E_1 = 00010000_2 00011100_2 00011010_2$,
  mis on sisendfailis 6. real.
- ... võtmega $K_2 = 10101010_2 10101010_2 10101010_2$
  saame küptogrami $E_2 = 11101111_2 11100011_2 11100101_2$,
  mis on sisendfailis 7. real.
- ... võtmega $K_3 = 11111111_2 11111111_2 11111111_2$
  saame küptogrami $E_3 = 10111010_2 10110110_2 10110000_2$,
  mis on sisendfailis 5. real.

Hindamine. Selles ülesandes on antud 10 sisendandmete komplekti failides `xortest.01.sis` kuni `xortest.10.sis` ja lahendusena on vaja esitada neile vastavad väljundandmete komplektid failides `xortest.01.val` kuni `xortest.10.val`. Programmi esitamine pole vajalik ja seda ei hinnata.