1. Alkulämmittelyksi:

a) Selväteksti SAUNA kryptautuu kryptotekstiksi

TAKE BACK VAT OR BONDS.

Mikä on kryptaus? (Periaatteessa mahdollisia kryptauksia on tietysti lukuisia, mutta se yksinkertaisin?)

b) Selväteksti SAUNAANDLIFE on kryptattuna

RMEMHCZZTCEZTZKKDA.

Mikä on kryptaus?

(Nämä tehtävät ovat akateemikko Arto Salomaan kirjasta, joka oli ensimmäisiä julkisen avaimen kryptauksen oppikirjoja ja vieläkin hyvin käyttökelpoinen. Salomaa on myös sauna-asiantuntija ja kirjassa on tarjolla runsaasti saunatietouttakin!)

2. Mitkä ovat ne kokonaisluvut x ja y, joille x:n jakaminen y:llä antaa osamäärän 5 ja jakojäännöksen 4?

3. Jaa y x:llä.

y	15	144	135	-115	-17
x	30	13	-8	-6	-20

4. Totea, että jos muotoa $11\cdots1$ oleva luku on alkuluku, niin sen pituus on myös alkuluku (esimerkiksi 11).

(Käänteinen ei päde yleisesti, esimerkiksi $111 = 3 \cdot 37$.)

5. Kirjoita desimaaliluku 3 000 **a)** 2-järjestelmään, **b)** 8-järjestelmään, **c)** 16-järjestelmään, **d)** 60-järjestelmään ja **e)** 100-järjestelmään.[1]

6. **a)** Jos muotoa $2^n - 1$ oleva luku (missä n on kokonaisluku) on alkuluku, niin n on myös alkuluku. Miksi? (*Vihje:* Geometrinen sarja

$$1 + 2^k + 2^{2k} + \cdots 2^{(l-1)k},$$

missä $n = kl$, liittyy asiaan. Vrt. myös Tehtävä **4**.)

(Nytkään käänteinen ei päde yleisesti, esimerkiksi $2^{11} - 1 = 2\,047 = 23 \cdot 89$. Nämä alkuluvut ovat ns. *Mersennen alkulukuja*.)

b) Suurin tunnettu tällainen alkuluku on

$$2^{57\,885\,161} - 1 = 581887266232246442175100 2\cdots 872574614198807172428 5951.$$

Mikä on sen pituus desimaaleissa?

(Tämä on myös suurin tällä hetkellä tunnettu alkuluku.)

[1] Mitkä ovat "tavallisimpien" pienten lukujärjestelmien suomenkieliset nimet? Ne ovat muodossa "järjestelmä (kantaluku, numeraaliyksikkö)": *binääri* (2, *bitti*), *ternääri* tai *trinääri* (3, *te(r)tti* tai *tritti*), *kvaternääri* (4, *(k)vartti* tai *kvatti*), *kvinääri* (5, *kvitti*), *senääri* (6, *setti*), *septenääri* (7, *septi*), *oktaali* (8, *okti* tai *oktaali*), *nonääri* (9, *nooni* tai *notti*), *desimaali* (10, *desimaali* tai *d(ig)itti*), *undenääri* tai *undesimaali* (11, *undesimaali*), *duodenääri* tai *duodesimaali* (12, *duodesimaali*), *heksadesimaali* (16, *heksadesimaali*), *vigesimaali* (20, *vigesimaali*), *seksagesimaali* (60, *seksagesimaali*), *sentenääri* (100, *sentti*) ja *millenääri* (1 000, *milli*).