Näidisülesandeid krüptoeksamiks

1. Defineeri/sõnasta:
   (a) korrutisšifri tõenäosusjaotus,
   (b) Diffie-Hellmani ülesanne,
   (c) libaalgarv,
   (d) jadašiffer.
2. Kirjelda järgmised algoritmid:
   (a) binaarmeetod modulaarseks astendamiseks,
   (b) sünnipäevarünne.
3. Digitaalsignatuurid. Motivatsioon (tavadokumentide võrdlus elektrondokumentidega ja sellest tulenevad nõuded). Signatuuriskeem. Lisaga ja sõnumit taastavad signatuuriskeemid. Signatuuriskeemide loomine avaliku võtme krüptosüsteemide baasil. Näited – RSA ja ElGamal.
4. Leia Silver-Pohlig-Hellmani algoritmi abil $\log_{14} 2$ rühmas $\mathbb{Z}_{17}^*$.
5. On teada, et arv 39203 on kahe algarvu korrutis. Tegurda see arv!
6. Tõesta, et iga kahe naturaalarvu k ja l korral kehtib seos
$$\gcd(k,l) \cdot \mathrm{lcm}(k,l) = k \cdot l.$$
Leia efektiivne algoritm kahe naturaalarvu vähima ühiskordse arvutamiseks.
7. Tõesta, et afiinsete kujutuste hulk
$$\{f : \mathbb{Z}_n \to \mathbb{Z}_n : x \mapsto k \cdot x + a \mid \gcd(k,n) = 1\}$$
on rühm kujutuste kompositsiooni suhtes.
8. Tuntud krüptograaf hr Kass mõtles välja järgmise isikutuvastusskeemi. Kõigepealt valib kasutaja oma salajaseks parooliks suure täisarvu n. Seejärel valib ta arvu $a \in \mathbb{Z}_n^*$, leiab Eukleidese algoritmi abil $a^{-1} \in \mathbb{Z}_n^*$ ja teatab tulevasele identifitseerijale (nt arvutisüsteemile) suurused a ja a^{-1}. Kui kasutaja soovib hiljem oma isikut tuvastada, teatab ta salajase suuruse n ning identifitseerija kontrollib, kas $a \cdot a^{-1} \equiv 1 \mod n$. Hinda selle süsteemi nõrkusi, kui ründaja
   (a) kuuleb pealt parooli ülekandmist;
   (b) pääseb ligi suurustrele a ja a^{-1}.
9. Tõesta, et kui m ja n on ühistegurita naturaalarvud, siis $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.