Võimalikke ülesannetetüüpe Krüptoloogia I 1. kontrolltöös 10. novembril 2005. aastal:

- Antud krüptosüsteem, (krüptimis)võti ja avatekst. Leida krüptotekst. Või siis on antud krüptosüsteem, (dekrüptimis)võti ja šiffertekst. Leida avatekst. Selleks võib tarvis olla näiteks järgmisi oskusi:
  - Hiina jäägiteoreem.
  - *Square-and-multiply* modulaarne astendamine.
  - Ruutjuure võtmine modulo algarv.
- Murda lahti krüptogramm, mille avatekstiks on mingi loomuliku keele tekst ja krüptosüsteemiks on kas *skytale*, nihkešiffer, afiinne šiffer või asendusšiffer.
- Teha kindlaks, kas kaks erineval viisil kirjeldatud krüptosüsteemi on tegelikult üks ja seesama krüptosüsteem. S.t. kas leidub mingi bijektsioon nende kahe süsteemi võtmeruumi vahel, nii et mõlema krüptosüsteemi kodeerimis- ja dekodeerimisfunktsioonid, võtmete hulgad ja tõenäosusjaotused nendel hulkadel oleksid samad?
- Arvutada entroopiaid ja tingimuslikke entroopiaid. Näiteks: antud on avatekstide ja võtmete hulgad ning tõenäosusjaotused neil. Samuti on antud kodeerimisfunktsioon. Leida $H(\mathbf{K}|\mathbf{C})$.
- Leida, mis on mingi etteantud funktsiooni $f : \{0,1\}^m \to \{0,1\}^n$ väljundXOR-ide tõenäosused, kui sisendXOR on ette antud. Kasutada seda infot võtme K leidmiseks, kui kodeerimisfunktsioon on kujul $e_K(x) = f(K \oplus x)$ (mingid avateksti-krüptoteksti paarid on ette antud).
- Leida lühim võimalik lineaarse tagasisidega nihkeregister, mis genereerib antud bitistringiga antud võtmejada.
- Leida, kas antud mitte liiga suure astmega polünoom üle $\mathbb{Z}_p$ (mitte liiga suure p jaoks) on taanduv või taandumatu. Kui ta on taandumatu, siis kas ta on ka primitiivne?
- Murda lahti krüptogramm, mille avatekstiks on mingi loomuliku keele tekst (sobival viisil arvudena kodeeritud) ja krüptosüsteemiks on kas seljakotisüsteem, RSA, Rabin või ElGamal, kusjuures parameetrid pole liiga suured.
- Arvutada Legendre'i / Jacobi sümbolite väärtusi.

- Arvutada diskreetseid logaritme mingites sobivalt valitud rühmades.
- Leida avatekst, kui on teada mitu erinevat RSA / Rabini krüptoteksti, mis talle vastavad, või siis on teada mitmele temaga lähedasele tekstile vastavad RSA / Rabini krüptotekstid.
- Mingitele avatekstidele vastavate RSA / Rabini / ElGamali krüptotekstide järgi konstrueerida nende avatekstidega teatud viisil seotud tekstile vastav RSA / Rabini / ElGamali krüptotekst.
- Näidata, et mingid lihtsad konstruktsioonid (näiteks suvaline kaheraundiline Feisteli šiffer) on ebaturvalised, või et ühe konstruktsiooni turvalisusest järeldub teise konstruktsiooni turvalisus (sarnaselt RSA osalise informatsiooniga).

Materjale võib kasutada.
Eeldatakse, et kontrolltöö lahendajal on kaasas mingi lihtne nelja tehet tegev kalkulaator (näiteks mobiiltelefon).