Kontrolltöö aines “Kodeerimine ja krüptimine”, I rühm

7.11.2001

1. (20 p) Olgu $\mathbf{M}$ multiplikatiivne, $\mathbf{N}$ nihke- ja $\mathbf{A}$ afiinne šiffer tähestikul Z_{26}. Olgu šifrite $\mathbf{M}$ ja $\mathbf{N}$ võtmeruumide tõenäosusjaotus ühtlane. Tõesta, et
$$\mathbf{N} \times \mathbf{M} \equiv \mathbf{A},$$
kusjuures saadud šifri võtmeruumi tõenäosusjaotus on ühtlane.

2. (10 p) Tõesta, et kui lineaarse tagasisidega nihkeregistri karakteristlik polünoom on $z^5 + z^2 + 1$, siis on selle LTNRi poolt genereeritud võtmejada perioodi pikkus 31.

3. (10 p) Analüüsi CBC-režiimis töötavat blokkšifrit, kui
   (a) $e_K(x) = K$,
   (b) $e_K(x) = x$.