Kontrolltöö aines "Kodeerimine ja krüptimine", II 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

   $$\mathbf{M} \times \mathbf{N} \equiv \mathbf{A},$$

   kusjuures saadud šifri võtmeruumi tõenäosusjaotus on ühtlane.

2. (10 p) Tõesta, et kui lineaarse tagasisidega nihkeregistri karakteristlik polünoom on $z^5 + z^3 + 1$, siis on selle LTNRi poolt genereeritud võtmejada perioodi pikkus 31.

3. (10 p) Analüüsi 16-raundise Feisteli šifri turvalisust, kui igas raundis kasutatakse sama alamvõtit ja raundifunktsioon töötab $f(R, K) = K$.