Povzetek

V prvem poglavju je opisan pomen kriptografije, definicija kriptosistema in uporaba v komunikacijskem kanalu. Temeljni cilj kriptografije je omogočiti dvema osebama, pošiljatelju in prejemniku, da komunicirata prek nezavarovanega kanala na tak način, da je nepooblaščenemu uporabniku sporočilo čim bolj nerazumljivo.

V drugem poglavju je predstavljenih sedem klasičnih kriptografskih sistemov, ki so jih ljudje uporabljali pred mnogimi leti. To so pomični, substitucijski ali Cezarjev, afin, Vigenerov, Hillov, permutacijski in tokovni sistem. Vsak sistem je predstavljen tudi s primerom.

Tretje poglavje pa se nanaša na analizo klasičnih kriptografskih sistemov. Sistemi so predstavljeni s primeri, kako lahko nepooblaščeni uporabnik prestreže določeno šifrirano besedilo. Analiziranih je pet sistemov: afin, substitucijski, Vigenerov, napad prvotnega besedila na Hillovem sistemu in kriptoanaliza tokovnega sistema na bazi LFSR.

Math. Subj. Class. (MSC 2000): 68P25, 94A60

Ključne besede:
kriptografija, kriptosistem, kriptoanaliza

Keywords:
cryptography, cryptosystem, cryptanalysis

Literatura

[1] B. Magajna. Tajnopisi. *Obzornik za matematiko in fiziko*, 38(1):9–18, april 1991.

[2] D. Stinson. *Cryptography: Theory and practice*. Chapman & Hall, 2002.

[3] J. Zupan. Nekaj o kriptografskih metodah. *Obzornik za matematiko in fiziko*, 25(4):129–136, julij 1978.