Uporaba javne kriptografije v inženirski praksi

Področje dela: matematika, kriptografija

Opis naloge:
Kriptografija je veda o varni komunikaciji po nezaščitenem kanalu. Pošiljatelj pred oddajo sporočilo šifrira (kodira). Prejemnik prejeto sporočilo dešifrira (dekodira). Kriptografija se opira na matematiko, predvsem na teorijo števil, logiko in statistiko. Ima dolgo in zanimivo zgodovino, ki sega v čas starih Egipčanov.

Ločimo simetrične (ali klasične) in asimetrične (ali javne) kriptosisteme. Pri simetričnih kriptosistemih je ključ en sam in je zato skrbno varovana skrivnost. Govorimo o tajnem ključu. Pri asimetričnih kriptosistemih pa je del ključa javno znan, del pa je zaseben. Prednost javnega kriptosistema pred simetričnim je v tem, da lahko pošiljamo šifrirana sporočila, ne da bi se prej zmenili za skrivni ključ. Varne in učinkovite javne kriptosisteme delimo v tri skupine: sistemi faktorizacije celih števil (npr. RSA), sistemi diskretnega logaritma (npr. DSA) in sistemi z eliptičnimi krivuljami.

V diplomski nalogi predstavite nekaj zgodovinsko najbolj znanih kriptografskih sistemov. Opišite teoretično osnovo javnih kriptosistemov, pri čemer se osredotočite na sisteme faktorizacije celih števil. Prikažite uporabo takega kriptosistema v inženirski praksi.

Literatura:
Johannes Buchmann: Introduction to cryptography, 2nd Edition, Springer, 2004.

Douglas Stinson: Cryptography : Theory and Practice, 3rd Edition, Chapman & Hall/CRC, Boca Raton, 2005.

A. Menezes, P. van Oorschot and S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1996.

Kontaktna oseba: doc. ddr. Melita Hajdinjak (e-naslov: melita.hajdinjak@fe.uni-lj.si)