Kryptologie

Ľubomíra Balková
lubomira.balkova@fjfi.cvut.cz

Katedra matematiky FJFI ČVUT v Praze

Nutnost šifrovat zprávy a zabránit tak nepříteli ve čtení soukromých informací je stará jako lidstvo samo. Od primitivních metod steganografie, kdy se sparťanským poslům holily hlavy, aby se na ně daly napsat tajné zprávy, a pak se čekalo, až jim vlasy dorostou, aby mohli vyrazit s tajnou informací na cestu, jsme se dnes posunuli do moderního světa, kde šifry chrání naše kreditní karty, zajišťují bezpečnost internetových plateb a pomocí digitálního podpisu zaručují pravost dokumentů. V SOČ práci se postupně podíváme na nejrůznější témata:

- Klasická kryptologie
  - Historické šifry
  - Šifrovací stroj - Lorenz
  - Šifrovací stroj - Enigma
- Generátory pseudonáhodných čísel a jejich aplikace v kryptografii
- Blokové symetrické šifry, DES a jeho kryptoanalýza - DES Cracker
- Testování prvočíselnosti
- Asymetrická kryptografie - RSA , ElGamal a DH , další metody
- Digitální podepisování pomocí asymetrické kryptografie
- Hašovací funkce - Algoritmus MD5 a SHA-3
- Kvantová kryptografie
- Kryptografie v praxi
  - Bezpečnost internetového bankovnictví, bankomaty, platební karty
  - Elektronický cestovní pas
  - Šifrování flash a jiných datových úložišť
  - Šifrování e-mailů
  - Bezpečnost mobilních telefonů

Studenti si budou také sami hledat informace na internetu a v literatuře, psát šifrovací a dešifrovací či dokonce kryptoanalytické programy. Postupně vznikne webová stránka s přehlednými informacemi o současném stavu kryptologie i její historii (především s odkazy na vhodné zdroje). Hlavním cílem SOČ práce bude vypracovat studii z jedné konkrétní oblasti, která studenta či studenty nejvíce zaujme. Tato studie by měla obsahovat nejen přehledný souhrn známých výsledků, ale i vlastní přínos, ať už ve formě vlastních programů či jiné.