Teorija kodiranja in kriptografija

Arjana Žitnik

Vsebina in cilji predmeta:

Kodiranje in kriptografija se uporabljata za zagotavljanje varne in zanesljive komunikacije ter hranjenje podatkov. Najbolj znana uporaba kriptografije je šifriranje podatkov, vendar je to le majhen delček sodobne kriptografije. Kode za popravljanje napak uporabljamo vsak dan, na primer pri uporabi mobilnega telefona, poslušanju glasbe na zgoščenkah, skeniranju kode QR...

Pri teoriji kodiranja bomo obravnavali naslednje teme: informacija in entropija; Shannonova teorija; kodi za popravljanje napak; zgornje meje za število kodnih besed; linearni, Hammingovi, ciklični in Reed-Solomonovi kodi, kodi QR.

Pri kriptografiji bomo obravnavali čim več tem izmed: klasična kriptografija; simetrični kriptosistemi; asimetrični kriptosistemi (kriptosistemi z javnim ključem), predvsem RSA; zgoščevalne funkcije; digitalni podpisi; distribucija in izmenjava ključev; identificiranje, overjanje in delitev skrivnosti; generiranje psevdo-naključnih števil; dokazi z ničelno informacijo.

Cilji predmeta so:

- spoznati osnovne tehnike sodobne kriptografije in teorije kodiranja, s poudarkom na matematični teoriji;
- spoznati osnove kriptoanalize: analiza varnosti in "razbijanje" preprostih kriptosistemov;
- razviti kritičnost pri uporabi komunikacijskih kanalov in računalniških sistemov s stališča informacijske varnosti.

Povezanost z drugimi predmeti:

Predmet je izrazito interdisciplinaren, z uporabo matemetičnih metod iz različnih področij: linearne algebre, teorije števil, algebre (grupe, končni obsegi, polinomi,...), verjetnostnega računa (diskretne slučajne spremenljivke, pogojna verjetnost in Bayesova formula) in računalništva (algoritmi, podatkovne strukture, računska zahtevnost).

Za uspešno spremljanje predmeta je potrebno, da je študent opravil oziroma posluša predmete *Algebra 1*, *Algebra 2*, *Uvod v programiranje* in *Verjetnostni račun* (začetni del). Vse potrebno predznanje bomo sproti obnovili.

Predmet ni pogoj za ostale predmete na 1. ali 2. stopnji študija matematike.

Izpitni režim:

- 2 kolokvija (ali pisni izpit) iz nalog,
- ustni izpit,
- ena obvezna domača naloga, ki jo bo potrebno rešiti s pomočjo računalnika (napisati bo treba računalniški program; zadošča znanje programiranja na nivoju predmeta *Uvod v programiranje*).
- Za sprotno delo bodo na voljo še neobvezne domače naloge, s katerimi si bo mogoče izboljšati oceno iz vaj - točke iz domačih nalog se prištejejo k točkam pisnega izpita.

Literatura:

- D. R. Stinson: *Cryptography : Theory and Practice*, 3rd edition, Chapman & Hall/CRC, Boca Raton, 2005.
- J. Talbot, D. Welsh: *Complexity and Cryptography*, Cambridge Univ. Press, Cambridge, 2006.
- D. Welsh: *Codes and Cryptography*, Oxford Univ. Press, Oxford, 1988.