Tečaj iz kriptografije in teorije kodiranja – 2003/04

PREDAVATELJ: Aleksandar Jurišić,
pisarna: Jadranska 19/III/308, tel.: 47-66-545, e-pošta: `fn11jurisic@uni-lj.si`

UČBENIKA: (za dodatne knjige, revije glej LITERATURO)
– D. R. Stinson, Cryptography – Theory and Practice, CRC Press, 2nd. ed., 2002.
– P. C. van Oorschot in S. A. Vanstone, An introduction to error correcting codes with applications, Kluwer Academic Publishers, 1989.

NAMEN: Pričelo se je vsesplošno komuniciranje in elektronsko trgovanje. Preko Interneta so dostopne številne podatkovne baze. Na vseh koncih se pojavljajo tudi pametne (čip) kartice, ki predstavljajo takorekoč računalnik v žepu. Z vsakim dnem bolj občutimo vpliv vsega tega na šolstvo, znanost ter družbo v širšem pomenu. Z razvojem telekomunikacij in obdelovanja informacij pa je tudi precej lažje prestreči in spremeniti digitalno informacijo kot pa njenega papirnega predhodnika, zato so se povečale zahteve po *varnosti*. **Informacijska in računalniška varnost** opisuje vse preventivne postopke in sredstva s katerimi zagotovimo dostop do informacijskih sistemov in njihovih ponudb ter preprečimo nepooblaščeno uporabo digitalnih podatkov ali sistemov, ne glede na to ali gre pri tem za *razkritje, spreminjanje, zamenjavo, uničenje* ustreznih podatkov ali *preverjanje verodostojnosti* informacij kot sta *digitalni denar* (nosilec vrednosti) in *digitalni podpisa* (za prepoznavanje). Med preventivnimi ukrepi nudi **kriptografija** največjo varnost oziroma zaščito glede na svojo prilagodljivost digitalnim medijem in s tem predstavlja osnovo informacijske družbe (cilji: zasebnost, celovitost podatkov, digitalno overjanje/podpisovanje, digitalni denar, in drugi kriptografski protokoli; obseg: matematika, računalništvo, elektrotehnika, finance, politika, vojska, itd.). Na vseh področjih komunikacij nastajajo standardi za kriptografsko zaščito (npr. IEEE, ANSI, ISO, IETF ipd).
Leta 1976 sta Diffie in Hellman predstavila koncept kriptografije javnih ključev, ki predstavlja nenadomestljivo orodje za poenostavitev upravljanja ključev ter realizacijo varne komunikacije. Od takrat naprej smo priča izrednemu povečanju aktivnosti na tem področju (prej pa so bile aktivnosti običajno omejene na takoimenovane črne kabinete). Kriptografske tehnike javnih ključev uporabljamo danes pri elektronski pošti, faksih, za zaščito proti virusom, pri digitalnem denarju, protokolih za internet, brezžičnih telefonih, kabelski televiziji, če omenimo samo nekaj primerov uporabe.
Večina kriptografskih sistemov je zasnovana na teoriji števil, povzročila pa je tudi odkritja novih algoritmov za stare probleme. Na tem tečaju bomo preučevali te nove algoritme teorije števil. Pri preučevanju varnosti oziroma pri napadih na kriptografkse protokole pa pogosto uporabljamo statistične principe. Spoznali bomo nekaj najbolj zvitih algoritmov in elegantne matematike nasploh. Namen tega tečaja je splošen uvod v kriptografijo in njeno zgodovino ter osvetlitev njenih pomembnejših dosežkov v zadnjih dvajsetih letih. Če bo čas dopuščal, bomo del tečaja posvetili teoriji kodiranja.

Obravnavali bomo čim več tem z naslednjega seznama:

- klasični tajnopisi, zgodovina kriptografije in Shannonova teorija
- Fiestelov tajnopis in AES (Advanced Encryption Standard)
- končni obsegi, razširjen Evklidov algoritem
- javni kriptosistemi, enosmerne funkcije in z njimi povezani problemi iz teorije števil (testiranje praštevilskosti, faktorizacija števil, diskretni logaritem) ter digitalni podpisi
- zgoščevalne funkcije in celovitost (integriteta) podatkov
- protokoli za izmenjavo ključev in za identifikacijo
- generatorji psevdonaključnih števil
- drugi protokoli (grb/cifra po telefonu, mentalni poker, sheme za delitev skrivnosti, kode za overjanje, vizualna kriptografija, dokaz brez znanja)
- infrastruktuara javnih ključev (PKI), agencija za overjanje (CA),
- teorija kodiranja

ter si ogledali nekaj filmov s področja kriptografije, računalniške varnosti in teorije kodiranja.

Matematično ozadje kriptografije predstavlja predvsem algebraična kombinatorika (vključno s teorijo števil), ki se uporablja še na dveh pomembnih področjih: v **teoriji statističnega designa** ter v **teoriji kodiranja**. Prva teorija išče optimalne množice vzorcev in se uporablja na primer za design digitalnih komunikacij. Drugo pa uporabljajamo pri nosilcih podatkov (npr. zgoščenkah) in prenosu podatkov (npr. brezžičnih napravah, satelitih), nemogoče/predrago je namreč preprečiti vse napake in jih zato raje sproti odpravljamo (npr. zgoščenka, ki ji zvrtamo luknjo premera 1mm, še vedno igra brezhibno). Teorija kodiranja se je razvila v zadnjih petdesetih letih in nam omogočila, da sestavimo sisteme, ki so kar se da zanesljivi (kolikor pač dopušča strojna oprema). Smatramo jo lahko za varnostno mrežo – matematično zavarovanje pred muhastim materialnim svetom, v katerem živimo.

DOMAČA STRAN: `http://valjhun.fmf.uni-lj.si/~ajurisic/tec3` bo vsebovala povzetke predavanj, kopije nekaterih prosojnic, reference za dodatno branje, kazalce na druge zanimive domače strani in še marsikaj, kar boste dodali vi.

DOMAČE NALOGE: Za utrjevanje snovi bo na voljo pet domačih nalog.

PROJEKTI: Opraviti bo treba seminarsko nalogo, ki bo vsebovala bodisi
- programiranje algoritma iz kriptografije in teorije števil,
- branje raziskovalnih/preglednih/zgodovinskih/ člankov iz kriptografije, algoritmične teorije števil, teorije kodiranja oziroma računalniške varnosti, ali
- neodvisno raziskovanje na tem področju.

(Lahko si izberete problem, ki ne bo na seznamu, vendar se predtem posvetujte s predavateljem.)

Končna ocena bo sestavljena iz ocen za domače naloge in seminarske naloge (pisni izdelek, krajša predstavitev v razredu in ustni zagovor).
Dodiplomci bodo lahko opravili namesto projekta pisni in ustni izpit.

Predznanje: dodiplomska matematika tehnične smeri, predvsem pa pripravljenost na individualno reševanje nalog oziroma programiranje kriptografskih algoritmov.

LITERATURA: (v matematični knjižnici ali pri predavatelju)

1. E. Bach and J. Shallit, Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, 1996. *[Zelo berljiva in podrobna knjiga, ki zajema osnovne algoritme iz teorije števil, vključno s testiranjem praštevilskosti, operacije v končnih obsegih in modularno aritmetiko.]*
2. H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993. *[Obsežna in pregledna knjiga o algoritmih iz teorije števil, testiranja praštevilskosti in faktorizacije števil.]* (SIG 6544/138)
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 2nd edition, 1994. *[Dober uvod v kriptografijo z vidika teorije števil. Šesto poglavje vsebuje tudi elementaren uvod v teorijo eliptičnih krivulj in v kriptosisteme z eliptičnimi krivuljami.]* (SIG 6544/114)
4. A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. *[Obsežen pregled moderne kriptografije z več kot 1000 citati literature.]* (SIG 11996/1)
5. P. C. van Oorschot in S. A. Vanstone, An introduction to error correcting codes with applications, Kluwer Academic Publishers, 1989.
6. B. Schneier, Applied Cryptography, Wiley, 2nd edition, 1996. *[Popularna knjiga o kriptografiji, namenjena širšemu krogu bralcev.]*
7. G. Simmons (editor), Contemporary Cryptology, IEEE Press, 1992. *[Zbirka preglednih člankov o raznih vidikih kriptografije.]*
8. D. Stinson, Cryptography: Theory and Practice, CRC Press, 2nd. ed. (1st part) 2002. *[Najnovejša knjiga o kriptografiji, ki je primerna kot učbenik]* (1. izdaja - SIG 11996/3)

REVIJE: Advances in Cryptology (Proceedings of CRYPTO, EUROCRYPT, and ASIACRYPT conferences); Journal of Cryptology; Designs, Codes and Cryptography; Cryptologia; IEEE Transactions on Information Theory; Mathematics of Computation.