KRIPTOGRAFIJA IN RAČUNALNIŠKA VARNOST

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

UČBENIK: Cryptography – Theory and Practice, Douglas R. Stinson, CRC Press, 3nd. ed., 2006. (glej LITERATURO za dodatne knjige, revije)

NAMEN: Nahajamo se na pragu vsesplošnega komuniciranja in elektronskega trgovanja. 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 *digitalnega 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 (na primer IEEE, ANSI, ISO, IETF in ATM Forum).

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.

Namen tega tečaja je splošen uvod v kriptografijo in osvetlitev njenih pomembnejših dosežkov v zadnjih dvajsetih letih. Obravnavali bomo čim več tem z naslednjega seznama:

- klasični tajnopisi in zgodovina kriptografije
- 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
- generator 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
- širši pogled na kriptografijo - varnost informacij ter varnost na mreži

ter si ogledali tudi nekaj filmov s področja računalniške varnosti.

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).

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

PROJEKTI: Opraviti bo treba seminarsko nalogo, ki bo vsebovala bodisi

- programiranje algoritma iz kriptografije in teorije števil
- neodvisno raziskovanje na tem področju ali
- branje raziskovalnih člankov iz kriptografije in algoritmične teorije števil.

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

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

Končna ocena bo sestavljena iz ocen za domače naloge in seminarske naloge (pisni izdelek, krajša predstavitev v razredu in ustni zagovor).

DOMAČA STRAN: `http://valjhun.fmf.uni-lj.si/~ajurisic/tec_fri6` bo vsebovala povzetke predavanj, kopije nekaterih prosojnic, reference za dodatno branje, kazalce na druge zanimive domače strani in se marsikaj, kar boste dodali vi.

LITERATURA: (v matematični knjižnici ali pri A.J.)

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. B. Schneier, Applied Cryptography, Wiley, 2nd edition, 1996.
   [Popularna knjiga o kriptografiji, namenjena širšemu krogu bralcev.]
6. G. Simmons (editor), Contemporary Cryptology, IEEE Press, 1992.
   [Zbirka preglednih člankov o raznih vidikih kriptografije.]
7. D. Stinson, Cryptography: Theory and Practice, CRC Press, 3nd. ed. (1st part) 2006.
   [Najnovejša knjiga o kriptografiji, ki je primerna kot učbenik] (1. izdaja - SIG 11996/3, 2. izdaja)

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