PROJEKTI

Opraviti bo treba seminarsko nalogo, ki bo vsebovala ali

- branje splošnih/poljudnih člankov iz kriptografije, teorije kodiranja in števil ter priprava sestavka, ki bi bil primeren za Presek, Uporabno informatiko, Monitor, Moj mikro, Delo oziroma druge podobne revije in časopise, ali
- branje raziskovalnih člankov iz kriptografije in algoritmične teorije števil ali
- neodvisno raziskovanje na tem področju ali
- programiranje algoritma iz kriptografije in teorije števil.

Lahko si izberete temo, ki je ni na seznamu, vendar se predtem posvetujte s predavateljem. Če si želite izbrati "realen" izziv, si lahko ogledate članek Adleman and McCurley, Open problems in number theoretic complexity, II Algorithmic Number Theory, Proc. 1st International Symposium, *ANTS-I*, Springer Lecture Notes in Computer Science, vol. 877 (1994), pp. 291-322. Toda velja opozorilo: ti problemi so verjetno zelo težki.

Eden od namenov tega projekta je tudi, da se naučite iskati reference na tem področju. Koliko (iskanja) informacij zadostuje? Če je vaš problem že dobro preštudiran in ste poiskali en sam vir (en članek ali knjigo), potem niste storili dovolj. (Tudi če članek *trdi*, da so našli končno rešitev, se morate o tem prepričati sami). Če ste zbrali več kot 10 člankov, potem morate nekako zožiti svoje področje, na primer tako, da zožite problem, ali način reševanja, ali pa da se osredotočite na najnovejša oziroma najbolj primerna dela.

Prav tako bi se morali ob projektu naučiti razpoznavati smiselnost rezultatov, ki jih imate na voljo in pretehtati, kateri so najbolj uporabni. Na koncu boste vse skupaj oddali v obliki seminarske naloge ter predstavili svoje rezultate v 15-20 minutnem nastopu v razredu.

Lista projektov (ki pa seveda še vedno ni dokončna - dopolnjevanje se nadaljuje):

1. V letu 1999 je bilo v ožji izbor izbiranih nekaj blokovnih šifer (Advanced Encryption Standard, kratica AES). Naredi pregled izbrancev in preuči kriterijev za njihov izbor.
   - `http://csrc.nist.gov/encryption/aes/aes_home.htm`,
   - `http://www.cl.cam.ac.uk/~rja14/`,
   - `http://www.mat.dtu.dk/persons/Jakobsen_Thomas/capapers.html`.

   Blokovne in tokovne šifre so primerljive. Zakaj?
   - Bruce Schneier, Crypto-Gram, January 15, 2000.

2. V marsikateri knjigi iz kriptografije ali pa poljudnem članku boste našli tudi slovarček osnovnih pojmov. (npr. ASCII, asymmetric-key cryptography, breaking of ciphers, cipher, cipher alphabet, cipertext, code, codebook, cryptoanalysis, cryptography, cryptology, decipher, decode, decrypt, DES, Diffie-Helman-Markle key exchange, digital signature, encipher, encode, encryption algorithm, key, key distribution, key escrow, key lenght, NSA, one-time pad, plaintext, PGP, private-key, public-key, public-key cryptography, quantum computer, quantum cryptography, RSA, steganography, substitution cipher, symmetric-key cryptography, transposition cipher, Vigenère cipher).

   Ali obstaja takšen slovenski slovarček? Poišči in dopolni ga oziroma naredi ga sam!

   Vsebovati bo moral večino kriptografskih izrazov iz našega učbenika in bo postavljen na našo domačo stran, da ga bomo lahko skupaj izboljševali.

3. Gemplus je ena izmed vodilnih podjetij za pametne kartice. Slovenija je svojo zdravstveno kartico naročila prav pri tem podjetju. Naredi analizo te kartice. V časopisu Delo je bilo napisanega kar nekaj o njej.

4. Brezžični telefoni (npr. Mobitel in Simobil) uporabljajo pametno kartico (GSM/Sim). Naredi analizo varnosti.
   - `http://www.zolatimes.com/v3.12/smartcards.htm`,
   - (cellular telephones c97-526 e97-239).

5. Ali je mogoče narediti prvo *domačo* pametno kartico? Kje naj začnemo? MS-toolkit, Certicom's Smart Card Toolkit?
   - Bruce Schneier, Crypto-Gram, January 15, 2000.
   - `http://www.zolatimes.com/v3.12/smartcards.htm`,
   - CryptoBytes
     `http://www.rsa.com/rsalabs/pubs/cryptobytes/html/article_index.html`.

6. Zgodovinska analiza kriptografije. Žal je to področje (tako kot mnoga druga) preobsežno, da bi ga predelali v celoti, zato se je potrebno osredotočiti na kaj konkretnega, npr. javno kriptografijo.
   - S. Singh, Code Book, The Science of Secrecy from Ancient Egipt to quantum Cryptography, Forth Estate Limited, London 1999 (MK 12932).
   - D. Kahn, The Codebreakers, The Story of Secret Writing, (hrvaški prevod: K. and M. Miles, Šifranti protiv špijuna, Centar za informacije i Publicitet, Zagreb 1979 ima 429+288+451+325=1493 strani).

7. Kaj lahko zvemo o NSA? Ali gre za *No Such Agency*? Kaj pa podobne agencije o drugih državah kot sta npr. Francija, Anglija?
   - S. Singh, Code Book, The Science of Secrecy from Ancient Egipt to quantum Cryptography, Forth Estate Limited, London 1999 (MK 12932).

8. Oglasna deska za tečaj kriptografije:
   (a) napiši program, ki nam bo omogočil, da se bodo na domačo stran prijavili samo registrirani poslušalci tečaja iz kriptografije, ali pa
   (b) zberi čim več materijala, ki bi bil primeren za našo domačo stran in ga spravi v elektronsko obliko.

9. Hackerji in crack programi.
   - `www.2600.com`,
   - Chaos Computer Club: `www.ccc.de`.

10. Portal Eon.si - Zakaj je kupovati v internetu varno?
    - `www.eon.si`. Ali jim verjameš?—.

11. Kaj je Echelon? Svetovni prisluškovalni sistem?
    - Jure Vižintin, Dan boja za zasebnosts: Sabotiranje zalezovalnega stroja, Delo, torek, 2. novembra, 1999, str. 4,
    - `http://www.europarl.eu.int/dg4/stoa/en/publi/default.htm`.

12. Kakšno zaščito imajo naše banke (SKB, NKBM, NLB-klik, KB),
    glej `http://www.geocities.com/Pentagon/Base/9107/`.

13. Zaščita parkingov z zapornicami (Ljubljani/Sloveniji) verjetno ni zelo močna.
    Testiraj varnost in možne napade.

14. Slovenska zakonodaja na področju kriptografije in računalniške varnosti.
    - `http://www2.arnes.si/~rzjtopl/slo/Merkur99.htm`,
    - `http://www.sigov.si/cvi/slo/ep/index.html`.

15. Kako lahko hitro generiramo tok ključev z veliko periodo? Posplošitev naloge 1.8 (Linear Feed Back Register) iz učbenika.

16. V naslednjem članku sta Kilian in Rogaway dokazala, da je DESX glede preverjanja vseh možnih ključev bistveno bolj varen kot DES:
    - J. Kilian and P. Rogaway, "How to protect DES against exhaustive key search", Advances in Cryptology – CRYPTO '96, pages 252-267.

17. Kleptografija (študij varne kraje informacij):
    - A. Young and M. Yung, "Kleptography: using cryptography against cryptography" Advances in Cryptology – EUROCRYPT '97, pages 62-74.
    - A. Young and M. Yung, "The prevalence of kleptographic attacks on discrete-log based cryptosystems" Advances in Cryptology – CRYPTO '97, pages 264-276.

18. Key escrow, kako skonstruirati kriptosistem javnih ključev v katerem bi vladalo ravnovesje med zasebnostjo posaneznikov (državljanov) ter ustavnim redom (ki naj bi ga zagotavljala država).

    - S. Micali, "Fair public-key cryptosystems" Advances in Cryptology – CRYPTO '92, pages 113-138.

    - J. Kilian and T. Leighton, "Fair cryptosystems, revisited" Advances in Cryptology – CRYPTO '95, pages 208-221.

19. Velika zahtevnost diskretnega logaritma na eliptični krivulji implicira veliko zahtevnost Diffie-Hellmanovega problema na eliptični krivulji. (Za ta projekt je potrebno poznati osnovne lastnosti eliptičnih krivulj.)
    - D. Boneh and R. Lipton, "Algorithms for black-box fields and their application to cryptography" Advances in Cryptology – CRYPTO '96, pages 283-297.

20. Spodnje meje za diskretne logaritme in sorodne probleme.
    (Netrivialne spodnje meje za splošni problem diskretnega logaritma v primeru, ko so grupni elementi naključno zakodirani in ko ima algoritem samo "omejen" dostop do grupne operacije.)
    - V. Shoup, "Lower bounds for discrete logarithms and related problems" Advances in Cryptology – EUROCRYPT '97, pages 256-266.

21. "Psevdo-naključno" generiranje števil v diskretnih algoritmih
    - M. Bellare, S. Goldwasser and D. Micciancio, ""Preudo-random" number generation within cryptographic algorithms: the DSS case", Advances in Cryptology – CRYPTO '97, pages 277-291.

22. Hitro odkrivanje potenc praštevil: Dan Bernstein, Detecting perfect powers in essentially linear time, `ftp://koobera.math.uic.edu/pub/papers/powers.dvi`

    V tem članku je uporabljen Loxtonov izrek o linearnih formah pri logaritmih. Posebno primeren bi bil za nekoga, ki ga zanima transcendentna teorija števil. Ali se lahko uporabi Bernsteinovo aplikacijo Loxtonovega izreka za rešitev naslednjega problema: za dana naravna števila a, b, c, i, j, k v polinomskem času odloči, če je $a^i b^j < c^k$.

23. Generator naključnih števil. Najboljša referenca za začetek je
    - Knuth, The Art of Computer Programming, Vol. 2.

    Lahko si ogledate tudi
    - G. Marsaglia and A. Zaman, A new class of random number generators, *Ann. Appl. Prob.* **1** (1991), 462-480.

24. Hitra metoda za računanje funkcije $\pi(x)$, ki določa število praštevil $\leq x$. Glej:
    - Lagarias and Odlyzko, Computing $\pi(x)$: An analytic method, *J. Algorithms* **8** (1987) 173-191;
    - Lagarias and Odlyzko, Computing $\pi(x)$: The Meissel-Lehmer method, *Math. Comp.* **44** (1985) FOCS.

25. Računanje z "nestandardno" predstavitvijo (zapisom) števil. Mnogi ljudje so za posebne namene predlagali uporabo verižnih ulomkov, aritmetike ostankov, p-adične aritmetike itd. Glej na primer
    - J. E. Vuillemin, Exact real computer arithmetic with continued fractions, *IEEE trans. Computers* **39** (1990), 1087-1105;
    - P. Kornerup and D. W. Matula, LCF: A lexicographic binary representation of the rationals, *J. Universal Comput. Sci.* **1** (7) (1995), 480-499.

26. Reševanje enačbe $x^2+ky^2 = m \pmod n$ v polinomskem času in njena uporaba za razbijanje sheme za digitalni podpis. Glej:
    - Pollard and Schnorr, An efficient solution of the congruence $x^2 + ky^2 = m \pmod n$, *IEEE Trans. Info. Theory*, **IT-33** (Sept. 1987), 702-709.

27. Izražanje števil kot vsote kvadratov in naključni polinomski čas. Glej:
    - Rabin in Shallit, Randomized algorithms in number theory, *Commun. Pure Appl. Math.* **39** (1986), S239-S256.

28. Metode algebraične geometrije, uporabljene za analizo algoritmov teorije števil. Glej npr.
    - E. Bach, Realistic analysis of some randomized algorithms, *J. Comput. Sys. Sci.* **42**, 30-53;
    - E. Bach and V. Shoup, Factoring polynomials using fewer random bits, *J. Symbolic Comput.* **9** (1990), 229-239.

29. Posebne arhitekture za faktorizacijo in druge probleme teorije števil. To je posebej zanimivo za tiste, ki jih zanima hardware. Glej:
    - Wunderlich, Factoring numbers on the massively parallel computer, Crypto '83, pp. 97-102;
    - Recent advances in the design and implementation of large integer factoring algorithms, IEEE Security & Privacy Conference (1983), pp. 2401-2405;
    - Wagstaff & Smith, An extended precision operand computer, Proc. 21st Southeast Region ACM Conference, 1983, pp. 209-216;
    - Pomerance, Smith, and Wagstaff, New ideas for factoring large integers, Crypto '83, pp. 81-85;
    - Pomerance, Smith, & Tuler, A pipeline architecture for factoring large integers with quadratic sieve algorithm, *SIAM J. Comput.* **17** (1988), 387-403.

30. Novi algoritmi za računanje diskretnega logaritma. Glej npr.
    - B. A. LaMacchia and A. M. Odlyzko, Computation of discrete logarithms in prime fields, *Designs, Codes, and Cryptography* **1** (1991), 47-62;

- A. M. Odlyzko, Discrete logarithm and smooth polynomials, in *Finite Fields: Theory, Applications, and Algorithms, Contemporary Mathematics* **168** (1994), 269-278,
- L. Adleman, J. DeMarrais and M. D. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, *Proc. ANTS-I*, 1994, 28-40;
- D. Gordon, Discrete logarithms in $GF(p)$ using number field sieve, *SIAM J. Discrete Math.* **6** (1993), 124-138.

Morda bo v naslednjih projektih dopisana se kakšna motivacija.

31. Algoritem za računanje števila p_n (n-tega praštevila) s pomočjo algoritma za računanje $\pi(x)$. ...

32. Računanje s kvantnim računalnikom (quantum cryptography c82-267 c84-475 e94-468 c95-424 c97-337: bit commitment c90-49, experiments e90-253 c96-329, key distribution c96-343, oblivious transfer c91-351 e95-133 c95-124).

33. DNA računanje, glej Scientific American...

34. Anonimnost (anonymity c81-138 c84-432 e85-241 e89-302 e89-320 e89-373 e89-690 e93-248 e94-332 e95-39 c96-61 e97-88 c97-395).

35. Napad s paradoksom rojstnih dnevov (birthday attack c85-14 e88-129 e96-307).

36. Timing attack (timing attacks c96-104, tamper resistance c83-387 c86-111 e87-83 c87-203 c87-216 c92-89 c93-456 c97-513).

37. Faktorizacija (factoring c83-71 c83-81 c83-87 c84-114 e85-31 e89-355 e91-281 e92-429: class group algorithm e82-325, elliptic curve algorithm c85-409 e92-183, Morrison-Brillhart algorithm e82-331, number field sieve c95-372, quadratic sieve c83-103 e84-169 e84-183, e88-235 e90-72 c92-324 c93-166 e93-28 e94-400, Schroeppel algorithm e82-331).

38. Varnost gesel (password security c81-81 e82-283 c87-392 c89-44, dynamic passwords e87-171).

39. Napad na RSAki uporablja lahke (tj. majhne) eksponente (low exponent attacks on RSA c85-403 e86-55 e89-372 e96-1 e96-155 e96-178).

40. Visualna kriptografija (visual cryptography e94-1 c96-401 c97-322).

41. Standardi (standards c81-39 e86-14 c87-3 c87-223 e89-267 c89-620 e91-547).

42. Zaščita programske opreme (software protection c81-79 e84-446 c85-140 c85-158 c86-426 c89-610 e90-474).

43. Digitalni/elektronski denar (electronic cash c91-338 c92-106 e94-156: anonymous cash c82-199 e88-107 c88-319 c89-481 c96-45 e95-121, divisible cash c91-324 e94-306 c95-438, double spending c93-292, off-line e93-318 c93-302, on-line e89-288, payment systems c82-187 c88-328 e89-294 e95-121, transferability e92-390).

Programerski projekt

Izberi si neko blok-šifro ali generator naključnih števil ali pa zgoščevalno funkcijo in opravi naslednje:

- podaj opis algoritma (referenca je lahko članek, knjiga, standard, Internet, Patenti, ...),
- poišči kodo na Internetu,
- oceni varnost (najboljši napadi, čas razbijanja, analiza statističnih lastnosti dobljenih zaporedij),
- oceni hitrost (algoritmično/asimptotično in časovno),
- opiši uporabo v kriptografiji in praksi,
- pripravi funkcijo kot objekt za Pascal (Delphi) oziroma C++ (Borland C++ Builder, MS Visual C++, GNU C++).

Nekateri **generatorji naključnih števil** (Random Number Generators):

1. Linear Feedback Shift Register (LFSR)
2. uporaba blok-šifer
3. uporaba zgoščevalnih funkcij (npr. SHA1)
4. potenciranje (kvadriranje)
5. večkratnik točke na eliptični krivulji

Nekatere **zgoščevalne funkcije**:

1. MD4, MD5,
2. SHA (other Name SHS), SHA1,
3. RipeMD128, RipeMD160, RipeMD256, RipeMD320,
4. Haval (128, 160, 192, 224, 256) with Rounds,
5. Snefru,
6. Square,
7. Tiger,
8. Sapphire II (128, 160, 192, 224, 256, 288, 320)
9. Checksums: CRC32, XOR32bit, XOR16bit, CRC16-CCITT, CRC16-Standard
10. HMAC

Nekatere **blok-šifre** (glej `http://www.hack.gr/users/dij/crypto/overview/otherbc.html`):

1. Gost,
2. Cast128, Cast256,
3. Blowfish,
4. IDEA
5. Mars,
6. Misty 1,
7. RC2, RC4, RC5, RC6,
8. FROG,
9. Rijndael,
10. SAFER (K40,...,K128,SK128),
11. TEA, TEAN,
12. Skipjack,
13. SCOP,
14. Q128,
15. 3Way,
16. Twofish
17. Shark,
18. Square,
19. Single DES, Double DES, Triple DES, (Double DES16, Triple DES16, TripleDES24, DESX), NewDES,
20. Diamond II, Diamond II Lite,
21. Sapphire II