Povzetek

Diplomsko delo predstavi matematične osnove ter osnovne kriptografske algoritme in protokole, ki temeljijo na problemu diskretnega logaritma in s pomočjo katerih lahko vzpostavimo sistem varne elektronske pošte. Ta temelji na kriptosistemih z javnimi ključi. Eden izmed osrednjih problemov je varen dogovor o ključu, ki sta ga razvila W. Diffie in M. Hellman. Za varen in učinkovit Diffie-Hellmanov dogovor o ključu uporabljamo praštevilske obsege. Protokol nad takim obsegom, ki temelji na problemu diskretnega logaritma, je ElGamalov protokol, s pomočjo katerega opišemo shemo digitalnega podpisa. Le-ta zagotavlja nedvoumno identiteto imetnika certifikata oz. digitalnega potrdila, celovitost podatkov, kar pomeni, da podatkov ni mogoče spremeniti ali drugače popraviti brez (vednosti) podpisnika. Podpisnik poleg tega ne more tajiti, da je on tisti, ki je podpisal poslano digitalno sporočilo. Certifikat povezuje podatke za preverjanje digitalnega podpisa z imetnikom in potrjuje njegovo identiteto. Certifikat je bistvena komponenta digitalnega podpisa, ki omogoča poslovanje preko spleta in ga izda za to pooblaščena, zaupanja vredna certifikatna agencija.

Math. Subj. Class. (MSC 2000): 11T71, 94A60, 68P25, 11A05, 11A07, 11A41

Ključne besede:
kriptografija, šifriranje, Evklidov algoritem, kongruence, primitivni elementi, praštevila, problem diskretnega logaritma, digitalni podpis, certifikat

Keywords:
cryptography, encryption, Euclidean algorithm, congruences, primitive roots, primes, discrete logarithm problem, digital signature, certificate

Literatura

[1] J. Budin in B. Batagelj, Varen prenos podatkov tudi po nevarnem omrežju, *Delo* 25. jan. (2007), 18.

[2] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Cliff Stein, Introduction to Algorithms (Second Edition), MIT Press, 2001.

[3] Taher ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, dostopno na `http://en.wikipedia.org/wiki/ElGamal_encryption`.

[4] A. Jurišić, Diffie-Hellmanov dogovor o ključu, *Presek* **34** (2006/2007), 25–30.

[5] A. Jurišić, Učno gradivo Kriptografija in teorija kodiranja 2003/2004, CD-ROM, Matematična knjižnica, ISBN 978-961-212-193-8
(dosegljivo tudi na `http://193.2.67.140/~ajurisic/tec3/`).

[6] A. Jurišić in J. Tonejc, Pametne kartice in varnost, 1. del, Zasebna življenja javnih ključev, 2. del, Napadi in obrambe: velike skrivnosti malih kartic, 3. del, *Monitor* **11**/6,7–8,9 (2001) 66–75, 44–53, 44–51.

[7] J. Keršnik, Varna elektronska pošta implementirana z uporabo OpenSSL, seminarska naloga, FRI, Univerza v Ljubljani, 2007.

[8] M. Mikac, Evidenca poštnih plačil v digitalni dobi, diplomsko delo, FMF, Univerza v Ljubljani, 2001.

[9] R. Petek, RSA kriptosistem, diplomsko delo, FMF, Univerza v Ljubljani, 2000.

[10] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, 1995.

[11] E. Schlegel, Pollardova ρ-metoda, magistrsko delo, FMF, Univerza v Ljubljani, 2003.

[12] S. Maksimovič, Učinkovitost aritmetike v praštevilskih obsegih in implementacija eliptičnih krivulj, diplomsko delo, FMF, Univerza v Ljubljani, 2003.

[13] I. Vidav, Algebra, Mladinska knjiga, Ljubljana, 1989.

[14] Simetrični kriptosistem AES dostopen na
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[15] Report on the Development of the Advanced Encryption Standard (AES),
http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf.

[16] Algoritem quicksort dostopen na
http://www.inf.fh-flensburg.de/lang/algorithmen/sortieren/quick/quicken.htm.

[17] Zgoščevalne funkcije (Cryptographic Hash Function) dostopne na
http://en.wikipedia.org/wiki/Cryptographic_hash_functions.

[18] Spletna stran certifikatne agencije Verisign dostopna na
http://www.verisign.com/repository/.

[19] Državni zbor RS, Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP),
http://www2.gov.si/zak/Zak_vel.nsf/4c1d8c547755fffac1256616002dd5e1/c12563a400338836c12568fd00505349?OpenDocument.

[20] Uporaba digitalnih potrdil v odjemalcu MS Outlook Express 5.0,
http://www.sigen-ca.si/nav-S-MIME-ie.php.

[21] Mozilla Thunderbird,
http://en.wikipedia.org/wiki/Mozilla_Thunderbird,
http://www.mozilla.com/en-US/thunderbird/.

[22] Protokol SSL, http://www.ca.gov.si/kripto/kr-ssl.htm.

[23] Mobilno plačevanje s sistemom M-Pay,
http://www.m-pay.com/index.php?lng=si.

[24] Mobilno plačevanje z Moneto, http://www.moneta.si/.

[25] Spletna stran podjetja Logos,
http://www.logos.si/Stran.aspx,
http://www.e-si.eu/?q=node/3.