POVZETEK

RSA kriptosistem spada med kriptositeme z javnimi ključi. Uporablja se za zagotavljanje zasebnosti in pristnosti podatkov. Varnost RSA kriptosistema temelji na težavnosti problema RSA in problema faktorizacije velikih števil. Diplomsko delo obsega opis, analizo in implementacijo RSA kriptosistema. Uvodni poglavji predstavita kriptografijo in matematična orodja, potrebna za razumevanje RSA kriptosistema. Tretje poglavje opiše RSA kriptosistem in njegovo uporabo v RSA šifrirni shemi in shemi RSA elektronskega podpisa. Sledi obravnava napadov na RSA kriptosistem in s tem povezane varnosti. Kot študent uporabne matematike sem poudarek posvetil implementaciji RSA kriptosistema. Poglavje o implementaciji vsebuje pregled algoritmov, ki sem jih uporabil pri programu "RSA Encrypter&Signer v1.0". Program je priložen diplomskemu delu na CD-ROM-u. Omogoča generiranje RSA ključev, šifriranje po RSA šifrirni shemi in elektronski podpis po shemi IFSSA, ki je del standarda IEEE P1363. Namen diplome je predstaviti bralcu pomembnost javne kriptografije, konkretno RSA kriptosistema, in mu z zgledom olajšati morebitno implementacijo tega ali kakega podobnega kriptosistema.

Ključne besede: RSA kriptosistem, napadi na RSA, implementacija RSA, kriptografija, šifriranje, elektronski podpis, Evklidov algoritem, kongruence, primitivni elementi, praštevila, faktorizacija, praštevilskost

Matematična predmetna klasifikacija (2000): 94A60, 68P25, 11A05, 11A07, 11A41, 11A51

ABSTRACT

RSA cryptosystem is a public-key cryptosystem. It provides privacy and ensures authenticity of digital data. Security of RSA cryptosystem is based on intractability of RSA problem and integer factorization problem. Diploma consists of description, analysis and implementation of RSA cryptosystem. First two chapters present cryptography and mathematical tools for understanding RSA cryptosystem. Third chapter describes RSA cryptosystem and it's use in RSA encryption scheme and RSA signature scheme. Chapter 4 focuses on attacks on RSA cryptosystem and related security. As a student of applied mathematics I emphasized the implementation of RSA cryptosystem. The chapter about implementation includes descriptions of algorithms, which were used to develop the enclosed software "RSA Encrypter&Signer v1.0". It supports generation of RSA keys, encryption with RSA encryption scheme and digital signature with IFSSA scheme, included in the IEEE P1363 standard. My main goal was to introduce the reader to public-key cryptography, in particular to RSA cryptosystem, and with my implementation aid eventual developers of this or any similar cryptosystem.

Key words: RSA cryptosystem, attacks on RSA, implementation of RSA, cryptography, encryption, digital signatures, Euclidean algorithm, congruences, primitive roots, primes, factorization, primality

Mathematics Subject Classification (2000): 94A60, 68P25, 11A05, 11A07, 11A41, 11A51

7. VIRI

[1] BACH, E., SHALLIT, J.: *Alghorithmic Number Theory, Volume I: Efficient Algorithms*, Mit Press, 1996.

[2] BONEH, D.: *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the American Mathematical Society, **46** (2), 1999, 203-213.

[3] BONEH, D., DURFEE G., FRANKEL, Y.: *An attack on RSA given a fraction of the private key bits*, ASIA-CRYPT '98, Lecture Notes in Computer Science, 1514, Springer-Verlag, 1998, 25-34.

[4] BONEH, D., DEMILLO, R., LIPTON, R.: *On the importance of checking cryptographic protocols for faults*, EUROCRYPT '97, Lecture Notes in Computer Science, 1233, Springer-Verlag, 1997, 37-51.
(glej http://ftp.cryptography.com/resources/papers/index.html)

[5] BONEH, D., VENKATESAN, R.: *Breaking RSA may not be equivalent to factoring*, EUROCRYPT '98, Lecture Notes in Computer Science, 1403, Springer-Verlag, 1998, 59-71.

[6] CHILDS, L.: *A Concrete Introduction to Higher Algebra*, Springer-Verlag, 1977

[7] COHEN, H.: *A Course in Computational Algebraic Theory*, Springer-Verlag, 1993.

[8] CONTINI, S.: *The factorization of RSA-140*, RSA Laboratories' Bulletin, **10**, 1999.
(glej http://www.rsasecurity.com/rsalabs/bulletins/)

[9] COPPERSMITH, D.: *Small solutions to polynomial equations and low exponent RSA vulnerabilities*, Journal of Cryptology, **10**, 1997, 233-260.

[10] COPPERSMITH, D., FRANKLIN, M., PATARIN, J., REITER, M.: *Low-exponent RSA with related messages*, EUROCRYPT '96, Lecture Notes in Computer Science, 1070, Springer-Verlag, 1996, 1-9.
(glej http://ftp.cryptography.com/resources/papers/index.html)

[11] DIFFIE, W., HELLMAN, M.E.: *New directions in cryptography*, IEEE Transactions on Information Theory, **22**, 1976, 644-654.

[12] HARDY, G.H., WRIGHT, E.M.: *An introduction to the Theory of Numbers*, Oxford Univ. Press, 1962.

[13] HASTAD, J.: *Solving stimultaneous modular equations of low degree*, SIAM Journal of Computing, **17**, 1988, 336-341.

[14] IEEE Standart Department: IEEE P1363 / D13 (Draft Version 13), *Standard Specifications for Public Key Cryptography*, 1999.
(glej http://grouper.ieee.org/groups/1363/index.html)

[15] JURIŠIĆ, A., TROJAR, A.: *Pametna kartica*, Uporabna informatika, **5**, 1997, 37-45.

[16] KAHN, D.: *The Codebreakers*, Macmillan Publishing Company, 1967.

[17] KOBLITZ, N.: *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987.

[18] KOCHER, P. C.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*, CRYPTO '96, Lecture Notes in Computer Sciences, 1109, Springer-Verlag, 1996, 104-113.
(glej http://ftp.cryptography.com/resources/papers/index.html)

[19] MENEZES, A., OORSCHOT, P., VANSTONE, S.: *Handbook of Applied Cryptography*, CRC Press, 1997.
(glej http://www.cacr.math.uwaterloo.ca/hac)

[20] PAPADIMITRION, C. H., STEIGLITZ, K.: *Combinatorial Optimization Algorithms and Complexity*, Prentice Hall Inc., 1982.

[21] RIVEST, R. L., SHAMIR, A., ADLEMAN, L.: *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM, **21** (2), 1978, 120-126.

[22] SHAND, M., VUILLEMIN, J.: *Fast Implementations of RSA Cryptography*, Proceedings of the 11th IEEE Symposium on Computer arithmetic, 252-259, 1993.

[23] STINSON, D. R.: *Cryptography - Theory and Practice*, CRC Press, 1995.

[24] VIDAV, I.: *Algebra*, Formatisk, 1989.

[25] WIENER, M.: *Cryptoanalysis of short RSA secret exponents*, IEEE Transactions on Information Theory 36, 1990, 553-558.