Povzetek

V tem delu je predstavljen ElGamalov kriptosistem za šifriranje v multiplikativnih grupah končnih obsegov. Definirana je eliptična krivulja in grupa na eliptični krivulji in v tem kontekstu je opisan ElGamalov kriptosistem. Vsi obravnavani pojmi so umeščeni v širši kriptografski okvir. Poleg tega so navedene osnove abstraktne algebre in teorije števil, s poudarkom na rezultatih, ki so pomembni za kriptografijo.

Ključne besede: eliptična krivulja, kriptografija, ElGamalov kriptosistem.

Abstract

In this thesis a description of ElGamal encryption in multiplicative groups of finite fields is given. Then, elliptic curves and elliptic groups are defined, and ElGamal encryption in this context is described. The cryptographic importance of the presented material is demonstrated. Also, an overview of basics of abstract algebra and elementary number theory with implications to cryptography is given.

Keywords: elliptic curves, cryptography, ElGamal cryptosystem

Math. Subj. Class. (2000): 68P25, 94A60, 11T71, 14H52.

Literatura

1. J. Barbič, *Schoofov algoritem*, Diplomsko delo, Univerza v Ljubljani, Fakulteta za matematiko in fiziko, 2000.
2. I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series. 265, Cambridge University Press, 1999.
3. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.
4. W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory **22** (1976), 644–654.
5. J. B. Fraleigh, *A First Course in Abstract Algebra*, 5th edition, Addison-Wesley, 1994.
6. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
7. IEEE P1363, *Standard Specifications for Public Key Cryptography*, Draft Version 13. Drafts available at `http://grouper.ieee.org/groups/1363`, 1999.
8. D. E. Knuth, *The Art of Computer Programming / Seminumerical Algorithms*, Volume 2, 3rd edition, Addison-Wesley, 1997.
9. N. Koblitz, *A Course in Number Theory and Cryptography*, GTM 114, Springer-Verlag, 1987.
10. J. López and R. Dahab, *An Overview of Elliptic Curve Cryptography*, Technical report, IC-00-10, May 2000. Available at `http://www.dcc.unicamp.br/ic-main/publications-e.html`.
11. A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.
12. National Institute of Standards and Technology, *Digital Signature Standard*, FIPS Publication 186-2, January 2000. Available at `http://csrc.nist.gov/fips`.
13. SEC1, *Elliptic Curve Cryptography*, Standards for Efficient Cryptography, September 2000, Version 1.0. Available at `http://www.secg.org`.
14. J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.
15. D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.
16. I. Vidav, *Algebra*, Društvo matematikov, fizikov in astronomov SRS, Ljubljana, 1987.
17. I. Vidav, *Eliptične krivulje in eliptične funkcije*, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 1991.