Povzetek

V tem delu bomo predstavili nov način evidentiranja plačila poštnine. V današnjem času se kot označba plačila uporablja predvsem poštna znamka. Odkar so se na trgu pojavili visoko zmogljivi tiskalniki, dostopni vsakomur, se je odpornost poštne znamke proti ponarejanju precej zmanjšala. Zato je nastala potreba po novem načinu evidentiranja plačila poštnine. Ta nov način predstavlja digitalna poštna znamka, ki jo bomo v tem delu podrobno predstavili. Spoznali bomo, iz katerih podatkov je sestavljena in raziskali način izdelave takih znamk. Ker bodo uporabljeni podatki precej zaupne narave, jih bomo zašifrirali. Da bi zagotovili pristnost uporabljenih podatkov, jih bomo podpisali z digitalnim podpisom. Tako se to delo ukvarja tudi s primernimi kriptografskimi protokoli. Uporabili bomo kriptografijo, ki temelji na eliptičnih krivuljah.

Ključne besede: digitalna poštna znamka, plačilo poštnine, digitalni podpis, eliptične krivulje.

Abstract

In this thesis a new way of evidencing postal payment is introduced. An example of such evidence of paid postage, which we use nowadays, is a post stamp. Ever since the inexpensive, high print quality computer printers appeared on the market, the resistance of post stamps against fraud was seriously damaged. So a new way of evidencing postal payment has to be introduced. The digital postal mark represents this new way. We will give a detailed description of such digital postal mark, learn all about the data which are taking part in such postal mark, and describe a way how to produce them. Because of the confidential nature of data used, we will encrypt them. Since we want to assure their authenticity, we will use a digital signature to sign them. Therefore we will also describe a corresponding cryptographic protocols. We will use cryptography based on elliptic curves.

Keywords: digital postal mark, postal revenue collection, digital signature, elliptic curves.

Math. subj. class(2001): 11T71, 11Y16, 11H52

Literatura

[1] D. R. L. Brown in D. B. Johnson, Formal Security Proofs for a Signature Scheme with Partial Message Recovery, Research Report CORR 2000-39, University of Waterloo (2000).

[2] R. Cordery, L. Pintsov, S. Vanstone, Cryptographic Postage Evidencing, preprint, 1996.

[3] A. Jurišić in A. J. Menezes, Elliptic Curves and Cryptography, *Dr. Dobbs Journal,* april 1997, 26-37.

[4] L. A. Pintsov in S. A. Vanstone, Postal Revenue Collection in the Digital Age, Research Report CORR 2000-43, University of Waterloo (2000).

[5] The United States Postal Service (USPS), Information-Based Indicia Program (IBIP), Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O), 23. 02. 2000. (`http://56.0.78.92/html/programdoc.html`).

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

[7] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: Handbook of Applied Cryptography, CRC Press 1997

[8] Elliptic Curve Online Tutorial, (`http://www.certicom.ca`).

[9] I. Vidav, Algebra, Mladinska knjiga, 1989.

[10] J. Barbič, Diplomska naloga: Schoofov algoritem, Fakulteta za matematiko in fiziko v Ljubljani, 2000.