(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 November 2002 (14.11.2002)

PCT

(10) International Publication Number
WO 02/091667 A1

(51) International Patent Classification⁷: H04L 9/30

(21) International Application Number: PCT/BY01/00006

(22) International Filing Date: 4 May 2001 (04.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and
(72) Inventor: MICHTCHENKO, Valentin Alexandrovich [BY/BY]; Nekrasova Strs., 28-210, Minsk, 220040 (BY).

(74) Agent: VINOGRADOV, Sergei Gennadievich; a/ya 114, Minsk, 220029 (BY).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/091667 A1

(54) **Title:** METHOD OF ENCRYPTING, TRANSMITTING AND DECRYPTING OF INFORMATION IN PUBLIC NETWORKS

(57) **Abstract:** Invention relates to a cryptographic method with the improved speed, in which the ecryption operations are performed with use of asymmetrical keys. A method for confidential transmitting messages includes preliminary encryption of message in such as manner that two independent parts are formed. The method is fast because only the short essential part of information is additionally encrypted by means of the public key. The stability of such encryption is much higher as compared with the use of separately taken methods because the core part, being encrypted by asymmetrical keys, is not subject to decrypting, since it has no semantic criterion.