PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{7} :
H04L 9/06

A1

(11) International Publication Number: **WO 00/65767**

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/BY99/00005

(22) International Filing Date: 27 April 1999 (27.04.99)

(71)(72) Applicant and Inventor: MISCHENKO, Valentin Alexandrovich [BY/BY]; 28–210, Nekrosova Str., Minsk, 220040 (BY).

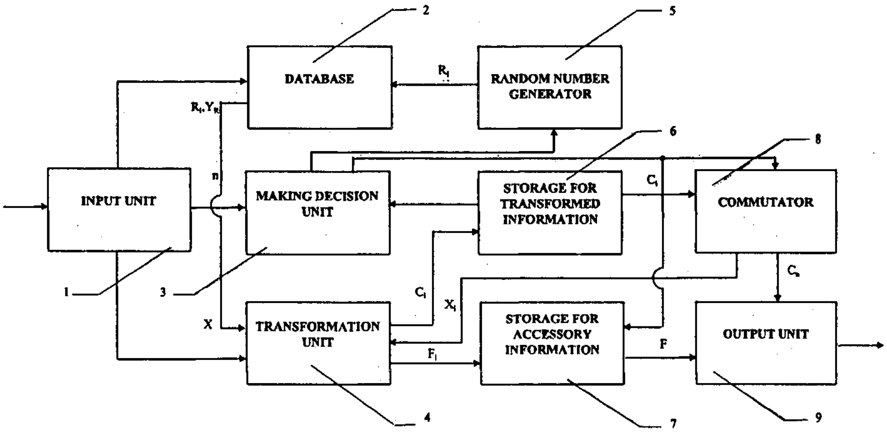
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ZAKHARAU, Uladzimir Uladzimirovich [BY/BY]; 1–2–22, 50 Let Pobedy Str., Minsk, 220056 (BY). VILANSKI, Yuri V. [BY/BY]; 10–44, Kuleshova Str., Minsk 220026 (BY). VERZHBALOVICH, Dzmitry I. [BY/BY]; Mvizru Pvo, Minsk 220057 (BY).

(74) Agent: VINOGRADOV, Sergei Gennadievich; P.O. Box 261, Minsk, 220006 (BY).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR ENCRYPTING INFORMATION AND DEVICE FOR REALIZATION OF THE METHOD



(57) Abstract

The invention relates to means for protecting information from an unauthorised access by electronic means. In order to transform the initial information the device has the transformation unit (4), the making decision unit (3), the storage of the recovered communication (6), the commutator (8), and for storing the accessory information the device has the storage of the accessory information (7). For encoding and transferring information the addressee is beforehand provided with a key to the received communications with information on regularities corresponding to the values of the communication transmitted to him, with specific values of the initial information for the whole set of symbols of the said kind of an information. In this case the addressee is beforehand provided with a set of transformation functions, Y_1, Y_2,..., $Y_N = Y_i,(X)$, where $X = \{x_1, x_2,..., x_m\}$ is a plurality of specific symbols of the transformed information. In the course of processing the encrypted information the input of the making decision unit (3) enters the information on the number (n) of transformation cycles of the initial communication. Before the beginning of the current transformation cycle, the making decision unit (3) transmits a control signal to the generator of random numbers (5), which generates a random number (Ri), transmits it to the data base (2) and through the latter to the transformation unit.