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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 April 2003 (03.04.2003)

PCT

(10) International Publication Number
WO 03/028281 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/CA01/01429

(22) International Filing Date: 15 October 2001 (15.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,358,048 25 September 2001 (25.09.2001) CA

(71) Applicant *(for all designated States except US)*: **3927296 CANADA INC.** [CA/CA]; 270 Albert Street, Ottawa, Ontario K1P 5G8 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **OOMMEN, John, B.** [CA/CA]; 5942 3rd Line Road, North Gower, Ontario K0A 2T0 (CA). **RUEDA, Luis** [AR/CA]; 360 Bell Street, Unit 1105, Ottawa, Ontario K1S 5E8 (CA).

(74) Agent: **MBM & CO.**; P.O. Box 809, Station B, Ottawa, Ontario K1P 5P9 (CA).

(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, EC, 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, PH, 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, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that 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 03/028281 A2

(54) Title: A CRYPTOSYSTEM FOR DATA SECURITY

(57) Abstract: A method and device for creating ciphertext from plaintext, and for decoding ciphertext, utilizing a tree structure for both encoding and decoding, the tree having leaves which are associated with plaintext symbols and the branches having assigned thereto a member of the ciphertext alphabet so that when encoding, a traversal is made between the root and the leaf corresponding to the plaintext and recording the ciphertext associated with each branch traversed, and when decoding, using the ciperhtext to determine the branches to be traversed until a leaf is reached and recording the plaintext associated with that leaf.