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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2001 (11.10.2001)

PCT

(10) International Publication Number
WO 01/76135 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/IB01/00103

(22) International Filing Date: 11 January 2001 (11.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00400912.2 3 April 2000 (03.04.2000) EP

(71) Applicant *(for all designated States except US)*: **CANAL+ TECHNOLOGIES SOCIETE ANONYME** [FR/FR]; 34, place Raoul Dautry, F-75516 Paris Cedex 15 (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BEUQUE, Jean-Bernard, Gerard, Maurice** [FR/FR]; 132, rue Victor Hugo, F-92270 Bois-Colombes (FR). **POULAIN, Philippe** [FR/FR]; 23, rue Alain Chartier, F-75015 Paris (FR).

(74) Agents: **COZENS, Paul, Dennis** et al.; Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, 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*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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 01/76135 A1

(54) Title: AUTHENTICATION OF DATA TRANSMITTED IN A DIGITAL TRANSMISSION SYSTEM

(57) Abstract: A method of authenticating data transmitted in a digital transmission system, in which the method comprises the steps, prior to transmission, of determining at least two encrypted values for at least some of the data, each encrypted value being determined using a key of a respective encryption algorithm, and outputting said at least two encrypted values with said data.