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

(19) World Intellectual Property Organization
International Bureau

G00002

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11362 A1

(51) International Patent Classification[7]: H04L 9/32, 29/06

(21) International Application Number: PCT/FI01/00689

(22) International Filing Date: 31 July 2001 (31.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20001734 1 August 2000 (01.08.2000) FI

(71) Applicant *(for all designated States except US)*: **NOKIA MOBILE PHONES LTD** [FI/FI], Keilalahdentie 4, FIN-02150 Espoo (FI)

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NIEMI, Valtteri** [FI/FI]; Tallberginkatu 3 as 43, FIN-00180 Helsinki (FI). **NIEMELÄ, Kari** [FI/FI], Loylykuja 3 as 2. FIN-90650 Oulu (FI) **HAMITI, Shkumbin** [YU/FI]; Leenankuja 2 K 115, FIN-02230 Espoo (FI). **SEBIRE, Guillaume** [FR/FI], Pursimiehenkatu 16 A 16, FIN-00150 Helsinki (FI).

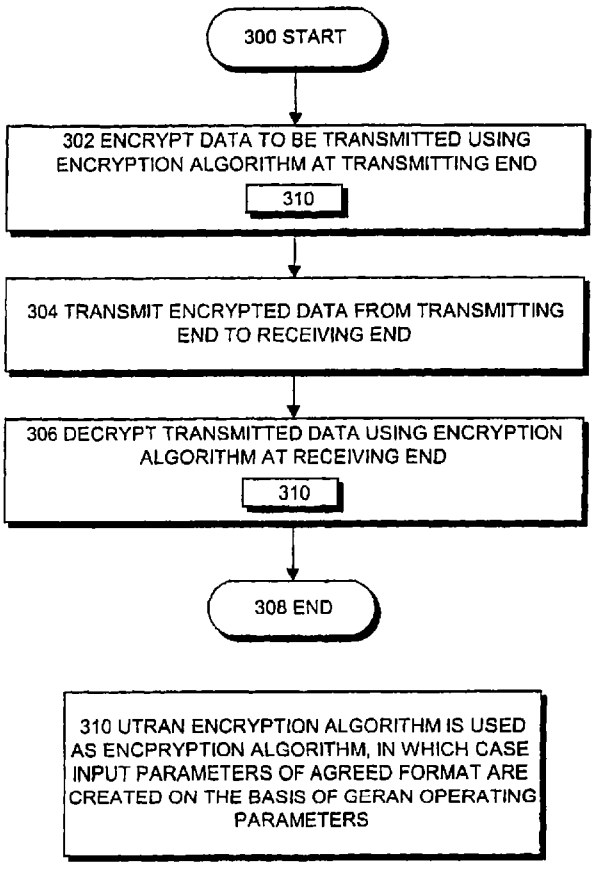
(74) Agent: **KOLSTER OY AB**, Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI)

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), 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, SK (utility model), 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

[Continued on next page]

(54) Title: DATA TRANSMISSION METHOD, USER EQUIPMENT AND GPRS/EDGE RADIO ACCESS NETWORK



(57) Abstract: The invention relates to a method for transmitting data between a GRPS/EDGE radio access network and user equipment of a mobile system, and to user equipment using the method, and to GERAN In the method, (302) the data to be transmitted in encrypted using an encryption algorithm at the transmitting end, (304) the encrypted data is transmitted from the transmitting end to the receiving end, and (306) the transmitted data is decrypted using an encryption algorithm at the receiving end. The used encryption algorithm is an encryption algorithm of the radio access network UTRAN employing the wideband code division multiple access method of the universal mobile telecommunications system, in which case the input parameters of agreed format required by the encryption algorithm are created on the basis of the operating parameters of the GPRS/EDGE radio access network GERAN.

162162

WO 02/11362 A1

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)

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

Published:

-- *with international search report*