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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2007 (19.04.2007)

PCT

(10) International Publication Number
WO 2007/044042 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2005/045399

(22) International Filing Date:
14 December 2005 (14.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/011,993 14 December 2004 (14.12.2004) US

(71) Applicant and
(72) Inventor: **MILLEVILLE, Dan, P.** [US/US]; 48 Groton School Road, Ayer, MA 01432-1000 (US).

(74) Agents: **CRONIN, Kevin, M.** et al.; Nutter McClennen & Fish LLP, World Trade Center West, 155 Seaport Boulevard, Boston, MA 02210-2604 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

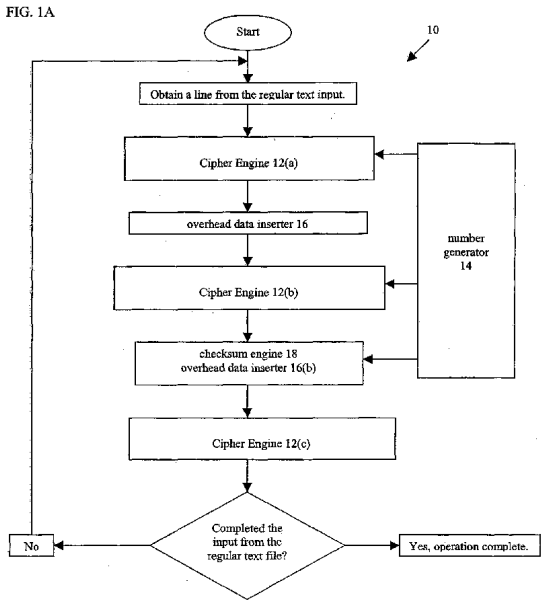
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
23 April 2009

(54) Title: ENCRYPTION METHODS AND APPARATUS

FIG. 1A



(57) Abstract: An encryption and decryption system is provided. The system includes multiple sub-key tables, each sub-key table associated with an identifying number and multiple cipher engines arranged serially, each cipher engine capable of executing a different encryption operation on an input data stream. The system also includes a number generator for generating numbers used to select sub-key tables. Data that assist deciphering engines with deciphering text encrypted with the cipher engines is inserted into the output data stream of at least one of the multiple cipher engines. The ciphering portion of the system alsoincludes a checksum engine positioned prior to the last cipher engine and adapted to produce a checksum value for insertion into the input data stream of the last cipher engine.

WO 2007/044042 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 05/45399

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/00 (2007.01)
USPC - 713/171
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 713/171

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/150, 171, 189, 190; 726/2, 5, 21; 380/44, 46, 277

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST(USPT,PGPB,EPAB,JPAB); Google Scholar
Search Terms: encryption, random, pseudo, number, sub-key, table, checksum, cipher, decipher, decryption, number generator, serial

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/0031050 A1 (Domstedt et al.) 18 October 2001 (18.10.2001), abstract, para [0014], [0030], [0032], [0049], [0053], [0081]-[0083], [0093], [0101], [0105], [0113], [0115], [0118], [0130]	1-26
A	US 2001/0021254 A1 (Furuya et al.) 13 September 2001 (13.09.2001)	1-26
A	US 6,570,989 B1 (Ohmori et al.) 27 May 2003 (27.05.2003)	1-26

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2007 (26.07.2007)	14 MAR 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)