PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L | A2

(11) International Publication Number: **WO 00/02340**

(43) International Publication Date: 13 January 2000 (13.01.00)

(21) International Application Number: PCT/US98/13626

(22) International Filing Date: 2 July 1998 (02.07.98)

(30) Priority Data:
09/108,312 1 July 1998 (01.07.98) US

(71) Applicant: TECSEC, INCORPORATED [US/US]; Suite 220, 1953 Gallows Road, Vienna, VA 22182 (US).

(72) Inventors: SCHEIDT, Edward, M.; 1048 Dead Run Drive, McLean, VA 22101 (US). WACK, C., Jay; 13715 Lewisdale Road, Clarksburg, MD 20871 (US).

(74) Agent: CHAMPAGNE, Thomas, M.; Rabin & Champagne, P.C., Suite 1111, 1725 K Street, N.W., Washington, DC 20006 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HR, HU, ID, IL, 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, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, 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, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: CRYPTOGRAPHIC COMMUNICATION PROCESS AND APPARATUS

(57) Abstract

A communication system, which includes an origination space, a communications channel, and a destination space associated with the origination space via the communications channel. The origination space includes an encryption engine for generating an output symbol O_t based on an input symbol I_t and means for receiving an encrypt key, an encrypt text/key relation, and the input symbol. The destination space includes a decryption engine for generating a decrypted symbol I'_t based on the output symbol received from the origination space via the communications channel and means for receiving a decrypt key and a decrypt text/key relation. The encrypt text/key relation controls the encryption engine such that $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{N-1}[\alpha_{N-2}(t) + ... + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]...]]$, mod W, where α_N, α_{N-1}, ..., α_1, α_0 are N+1 additive transformations defined by the encrypt key, where π_N, π_{N-1}, ..., π_2, π_0 are N permutations defined by the encrypt key, and where W represents the number of possibilities for each permutation defined by the encrypt key. The decrypt text/key relation controls the decryption engine such that $I'_t = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1} ...[\pi_{N-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - ... - \alpha'_3(t)] - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, where π_i^{-1} is defined by the decrypt key as the inverse of the permutation π_i, where α'_N, α'_{N-1}, ..., α'_1, α'_0 are N+1 additive transformations defined by the decrypt key, and where W represents the number of possibilities for each inverse permutation defined by the decrypt key.

