Title (en)

CRYPTOGRAPHIC METHOD USING A DATA FLOW-SYMMETRICAL CRYPTOGRAPHIC ALGORITHM AND USE IN A SMART CARD

Title (de)

KRYPTOGRAPHISCHES VERFAHREN UNTER VERWENDUNG EINES SYMMETRISCHEN STROMVERSCHLÜSSELUNGSALGORITHMUS UND ANWENDUNG FÜR EINE CHIPKARTE

Title (fr)

PROCEDE DE CRYPTOGRAPHIE UTILISANT UN ALGORITHME CRYPTOGRAPHIQUE SYMETRIQUE PAR FLOT ET APPLICATION A UNE CARTE A PUCE

Publication

EP 1479189 A1 20041124 (FR)

Application

EP 03717411 A 20030218

Priority
• FR 0300532 W 20030218
• FR 0202226 A 20020221

Abstract (en)

[origin: WO03071735A1] The invention concerns a cryptographic method using a data block-symmetrical cryptographic algorithm such as DES in a particular sequence enabling its cryptographic strength to be increased significantly. Said method enables generating a pseudo-random number, and/or a strong random variable or data flow encryption/decryption and/or authentication of messages to be generated. It is more particularly adapted to encryption/decryption and to authentication by a smart card of data contained in a remote memory.

IPC 1-7

H04L 9/32

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP)

H04L 9/0637 (2013.01); **H04L 9/0662** (2013.01); **H04L 9/50** (2022.05)

Citation (search report)

See references of WO 03071735A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR

DOCDB simple family (publication)

WO 03071735 A1 20030828; AU 2003222578 A1 20030909; EP 1479189 A1 20041124; FR 2836311 A1 20030822; FR 2836311 B1 20040528

DOCDB simple family (application)

FR 0300532 W 20030218; AU 2003222578 A 20030218; EP 03717411 A 20030218; FR 0202226 A 20020221