Title (en)

CRYPTOGRAPHIC ENGINE USING BASE CONVERSION, LOGIC OPERATIONS AND PRNG IN DATA ARRAYS TO INCREASE DISPERSION IN CIPHERTEXT

Title (de)

KRYPTOGRAPHISCHE VORRICHTUNG UNTER VERWENDUNG EINER BASISUMWANDLUNG, LOGISCHE OPERATIONEN UND ZUFALLSZAHLENGENERATOR IN EINEM DATENFELD ZUR VERGRÖSSERUNG DER DISPERSION IN EINEM VERSCHLÜSSELTEN TEXT

Title (fr)

MOTEUR CRYPTOGRAPHIQUE UTILISANT LA CONVERSION DE BASE DE NUMERATION, DES OPERATIONS LOGIQUES ET UN GENERATEUR DE NOMBRES PSEUDO-ALEATOIRES POUR DES MATRICES DE DONNEES DE FA ON A AUGMENTER LA DISPERSION DANS LE TEXTE CHIFFRE

Publication

EP 1179243 A4 20050720 (EN)

Application

EP 99927081 A 19990518

Priority

US 9910967 W 19990518

Abstract (en)

[origin: CA2371452A1] The plaintext is partitioned, block-by-block, the block size being a user selectable power of 2 in size (step 1). The data bytes in the input block ar e selected M bytes at a time, where M >= 2, with permuted addressing to for m a single concatenated data byte, CDB. The CDB is modified by rotating (or barr el shifting) a random bit distance (step 7). The CDB may also be modified befor e or after rotation by simple arithmetic/logic operations (step 12). After modification, the CDB is broken up into M bytes and each of the M bytes is placed into the output block with permuted addressing (step 4). The output block, or ciphertext, may again be used as an input block and the process repeated with a new output block. This scheme may be used as an encryption method by itself or in conjunction with other block encryption methods. The latter may be accomplished by using this scheme between successive stages of other encryption methods on blocked data, or between an internal stage of th e other methods. The sources of random number (step 2) used to determine the distance for the random rotation operation can be from: a pseudo-random numb er generator, sampled music CD-ROMs, entries in tables arrays, buffers, or any other digital source.

IPC 1-7

H04L 9/28

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/06** (2006.01)

CPC (source: EP)

H04L 9/0618 (2013.01); **H04L 9/0662** (2013.01); H04L 2209/04 (2013.01); H04L 2209/12 (2013.01)

Citation (search report)

- [X] SCHNEIER, B.: "Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition", 1996, JOHN WILEY & SONS, INC., NEW YORK, XP002329180, 218930
- [X] RIVEST R L: "THE RC5 ENCRYPTION ALGORITHM", FAST SOFTWARE ENCRYPTION. INTERNATIONAL WORKSHOP, 1995, pages 86 - 95, XP000890159
- See references of WO 0070819A1

Cited by

CN113542196A

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)

CA 2371452 A1 20001123; EP 1179243 A1 20020213; EP 1179243 A4 20050720; JP 2003500681 A 20030107

DOCDB simple family (application)

CA 2371452 A 19990518; EP 99927081 A 19990518; JP 2000619156 A 19990518