Title (en)

METHOD FOR CALCULATING A CRYPTOGRAPHIC KEY CONTROL DATUM

Title (de)

VERFAHREN ZUR BERECHNUNG EINER KONTROLLINFORMATION EINES KRYPTOGRAPHISCHEN SCHLÜSSELS

Title (fr)

PROCEDE DE CALCUL D'UNE DONNEE DE CONTROLE DE CLE CRYPTOGRAPHIQUE

Publication

EP 1277306 A1 20030122 (FR)

Application

EP 01927998 A 20010418

Priority

- FR 0101194 W 20010418
- FR 0005254 A 20000425

Abstract (en)

[origin: WO0182525A1] The invention concerns a method for calculating a control datum of a secret key algorithm with N bits, including N-N/n random and encryption bits and N/n checksum bits. The invention is characterised in that it comprises the following steps: encrypting a specific message of K bits using N/n encryption bits of the key; constructing a control datum by selecting N/n bits among the K bits of the encrypted message; integrating one of the N/n bits of said control datum in all the n-1 encryption bits so as to constitute a complete secret key of N bits. The invention is particularly applicable to the data encryption standard (DES), the control datum being constructed from a constant message.

IPC 1-7

H04L 9/06

IPC 8 full level

H04L 9/06 (2006.01)

CPC (source: EP US)

H04L 9/004 (2013.01 - EP US); **H04L 9/0625** (2013.01 - EP US); H04L 2209/08 (2013.01 - EP US)

Citation (search report)

See references of WO 0182525A1

Designated contracting state (EPC)

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

DOCDB simple family (publication)

WO 0182525 A1 20011101; AU 5487701 A 20011107; CN 1426645 A 20030625; EP 1277306 A1 20030122; FR 2808145 A1 20011026; FR 2808145 B1 20020927; US 2003103625 A1 20030605

DOCDB simple family (application)

FR 0101194 W 20010418; AU 5487701 A 20010418; CN 01808481 A 20010418; EP 01927998 A 20010418; FR 0005254 A 20000425; US 25713002 A 20021009