Title (en)

ENCRYPTION METHOD AND APPARATUS WITH VARIABLE ENCRYPTION STRENGTH

Title (de)

VERFAHREN UND VORRICHTUNG ZUR VERSCHLÜSSELUNG MIT VARIABLER VERSCHLÜSSELUNGSSTÄRKE

Title (fr)

PROCEDE ET APPAREIL A PUISSANCE DE CRYPTAGE VARIABLE

Publication

EP 1016239 A1 20000705 (EN)

Application

EP 98942910 A 19980914

Priority

- GB 9802774 W 19980914
- GB 9719726 A 19970916

Abstract (en)

[origin: GB2329308A] An encryption method and apparatus in which a cryptographic encryption key K for use to encrypt or decrypt communications is first derived from a cryptographic key Kd provided by a user. The derived encryption key is used to encrypt or decrypt communications at a selected level of encryption strength. The level of encryption strength is selected in accordance with whether or not the cryptographic key provided by the user has a particular property, such as including a particular sequence of bits, dividing exactly by a particular number, or whether a particular cryptographic check value S can be derived from it. This method prevents unauthorised users from using the apparatus at full encryption strength since the key they provide will probably not have the required properties or generate the required check value. Also described is a method and apparatus for generating a certified cryptographic key by combining the user key Kd with a check value derived from it.

IPC 1-7

H04L 9/08

IPC 8 full level

H04L 9/08 (2006.01)

CPC (source: EP)

H04L 9/088 (2013.01)

Citation (search report)

See references of WO 9914887A1

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)

GB 2329308 A 19990317; **GB 2329308 B 20000209**; **GB 9819988 D0 19981104**; AU 9087598 A 19990405; CN 1277769 A 20001220; EP 1016239 A1 20000705; GB 9719726 D0 19980318; IL 135080 A0 20010520; WO 9914887 A1 19990325; ZA 988391 B 20000322

DOCDB simple family (application)

GB 9819988 A 19980914; AU 9087598 A 19980914; CN 98810547 A 19980914; EP 98942910 A 19980914; GB 9719726 A 19970916; GB 9802774 W 19980914; IL 13508098 A 19980914; ZA 988391 A 19980914