Title (en)

METHOD FOR MAKING SECURE THE TRANSMISSION OF A MESSAGE FROM A TRANSMITTING DEVICE TO A RECEIVING DEVICE

Title (de)

VERFAHREN ZUR SICHERUNG DER ÜBERTRAGUNG EINER NACHRICHT VON EINER SENDEVORRICHTUNG ZU EINER EMPFANGSVORRICHTUNG

Title (fr)

PROCEDE DE SECURISATION DE LA TRANSMISSION D'UN MESSAGE D'UN DISPOSITIF EMETTEUR A UN DISPOSITIF RECEPTEUR

Publication

EP 1040620 A1 20001004 (FR)

Application

EP 98962482 A 19981216

Priority

- FR 9802753 W 19981216
- FR 9715971 A 19971216

Abstract (en)

[origin: FR2772532A1] The invention concerns a method for making secure the transmission of a message (Prgm) from a transmitting device (E) to a receiving device (R), characterised in that: the message (Prgm) is split into n elementary units (I), n being a number not less than 1; a logical property (P) is defined such that, for each elementary unit (I), the logical property (P), applied to an authentic elementary unit (I), gives a true logical value; the message (Prgm) is encrypted by the transmitting device (E) encryption means using an encryption algorithm comprising a key (Kc) so as to obtain a result Kc(Pgrm); The encrypted result Kc(Pgrm) is transmitted by the transmitting device (E) to the receiving device (R); the encrypted result Kc(Pgrm) is decrypted by the receiving device (R) using a decryption algorithm comprising a secret key (Kd) so as to obtain a decrypted result Kd(Kc(Pgrm)); the decrypted result Kd(Kc(Pgrm)) is split into elementary units (I); the logical property (P) is applied to the elementary units (I) so as to obtain, for each unit, a true logical value or a false logical value. The method is particularly applicable to smart cards.

IPC 1-7

H04L 9/32; G06F 12/14; G06F 1/00

IPC 8 full level

G06K 19/07 (2006.01); **G06F 1/00** (2006.01); **G06F 21/60** (2013.01); **G06K 17/00** (2006.01); **G09C 1/00** (2006.01); **H04L 9/10** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

G06F 21/606 (2013.01); **H04L 9/32** (2013.01); G06F 2211/007 (2013.01)

Citation (search report)

See references of WO 9931845A1

Designated contracting state (EPC)

DE ES FR GB

DOCDB simple family (publication)

FR 2772532 A1 19990618; **FR 2772532 B1 20000107**; CN 1284227 A 20010214; EP 1040620 A1 20001004; JP 2002509269 A 20020326; WO 9931845 A1 19990624

DOCDB simple family (application)

FR 9715971 A 19971216; CN 98813288 A 19981216; EP 98962482 A 19981216; FR 9802753 W 19981216; JP 2000539611 A 19981216