Title (en)

SYSTEM, DEVICE AND METHOD FOR SECURE COMMUNICATION AND ACCESS CONTROL

Title (de)

SYSTEM, VERFAHREN UND VORRICHTUNG ZUR SICHEREN KOMMUNIKATION UND ZUGANGSKONTROLLE

Title (fr)

SYSTEME, DISPOSITIF ET PROCEDE POUR COMMUNICATION ET COMMANDE D'ACCES SECURISEES

Publication

EP 1166491 A2 20020102 (EN)

Application

EP 99973795 A 19990623

Priority

- US 9914224 W 19990623
- US 10401498 A 19980624
- US 30987399 A 19990511

Abstract (en)

[origin: WO0067548A2] A method for generating an identical electronic one-time pad at a first location and at a second location, the method comprising the steps of: (a) providing a first electronic device at the first location and a second electronic device at the second location, each of the first and the second electronic devices having: (i) a non-volatile memory; (ii) a processor; (iii) at least one table of true random numbers being stored on the non-volatile memory, the table being identical for the first and the second electronic devices; and (iv) at least one software program for obtaining a true random number from the table, the software program being stored on the non-volatile memory and the at least one software program being operated by the processor; (b) providing a communication channel for communication between the first electronic device and the second electronic device; and (c) selecting a selected true random number from the table at the first and the second electronic devices according to a selection procedure, the selection procedure being identical for the first and the second electronic devices, the selection procedure including exchanging at least a portion of a key between the first and the second electronic devices over the communication channel, such that the selected true random number is identical for the first and the second electronic devices; and (d) forming at least a portion of the identical electronic one-time pad at the first and the second locations with the selected true random number. The identical electronic one-time pad is of any desired length. There is also provided a method for generating a practically unlimited quantity of true random numbers, the true random numbers being identical in a plurality of locations, the method being operable by a data processor and the method comprising the steps of: (a) providing an identical table of true random numbers, an identical pointer, an identical seed and an identical pseudorandom number generator at each of the plurality of locations; (b) obtaining an obtained true random number from the identical table of true random numbers according to the pointer, the obtained true random number being identical at the plurality of locations; (c) generating a generated pseudorandom number by the pseudorandom number generator, the generated pseudorandom number being identical at the plurality of locations; and (d) combining the obtained true random number and the generated pseudorandom number to form at least one of the quantity of true random numbers, the at least one of the quantity of true random numbers being identical at the plurality of locations. In addition, the present invention includes a "star" network system, in which a central electronic device has a master table and a plurality of customer electronic devices each have at least one table stored in two forms, both a form which is encrypted according to this master table and a non-encrypted form. The customer electronic device then sends this encrypted table to the central electronic device, which decrypts the table in order to initiate communication.

[origin: WO0067548A2] A method is disclosed for generating an identical electronic one-time pad at a first and second locations. Each location is provided an electronic device, said electronic devices containing identical tables of true random numbers. In order to select an identical one-time pad at the first and second locations using the provided electronic devices, a portion of a key is exchanged between the two devices via a communications network, and is subsequently used as a pointer to select a true random number from the tables at the first and second devices. At least a portion of the one-time pad is formed with the true random number selected from the table. Also disclosed is a method for generating a practically unlimited quantity of true random numbers being identical at a plurality of locations through the addition of pseudorandom number generators to the electronic devices. The invention may also be implemented in a network setting wherein a central electronic device has a master table and a plurality of customer devices each have at least one table stored in two forms: one encrypted according to the master table and one in non-encrypted form. The customer electronic device then sends this encrypted table to the central electronic device, which decrypts the table in order to initiate communications.

IPC 1-7

H04L 9/00

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/20** (2006.01)

CPC (source: EP)

H04L 9/0656 (2013.01); **H04L 9/0838** (2013.01); H04L 2209/08 (2013.01)

Citation (search report)

See references of WO 0067548A2

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)

WO 0067548 A2 20001116; **WO 0067548 A3 20010809**; AU 6887800 A 20001121; CA 2347659 A1 20001116; EP 1166491 A2 20020102; JP 2002544690 A 20021224

DOCDB simple family (application)

US 9914224 W 19990623; AU 6887800 A 19990623; CA 2347659 A 19990623; EP 99973795 A 19990623; JP 2000616599 A 19990623