

ABSTRACT**Cryptographic method for securely exchanging messages and
device and system for implementing this method**

5

The present invention refers to a method for securely exchanging messages (M) between at least two devices (D1, D2) each storing a shared secret key (K), comprising the steps of:

at each device:

10

- generating a random number (R1, R2), then sending it to the other devices,

- determining a first key (K1) by a first operation based onto said secret key and each random number,

15

- determining a second key (K2) based on said first key and said random numbers,

at a sending device (D1):

- determining a pseudo message (M') on the basis of the message (M) and said random numbers,

20

- calculating then sending a cryptogram (C) on the basis of said pseudo message (M') and said second key (K2),

at the receiving device (D2):

- decrypting said cryptogram (C) by means of said second key, then

- retrieving said message (M) from said pseudo message (M').

(Fig. 2)

25