ABSTRACT

This invention relates to a method for transmitting messages between an emitter and at least one receiver, comprising the following steps :

- encryption of the message (m) to be transmitted by means of a key (a) associated to said emitter;
- sending of the encrypted message in a conversion module comprising a conversion key ($\pi_{a\to b}$) and a conversion function;
- conversion of the encrypted message received in the conversion module in an encrypted message in order to be able to be decrypted by a key (b) specific to said receiver, this conversion being carried out without the initial message appearing in plaintext in the conversion module;
- sending the converted message to said receiver;
- decryption of said transformed message received by said receiver by means of the specific key b;

characterized in that the conversion key ($\pi_{a\to b}$) of the conversion module depends on a non trivial value raised to the power of the key (a) bound to the emitter and of the key (b) bound to the receiver.

This invention also relates to a system for transmitting messages between an emitter and at least one receiver, this system being arranged to implement the method of the invention.