INFORMATION ENCRYPTING TRANSMISSION AND RECEPTION METHOD

ABSTRACT

PROBLEM TO BE SOLVED

To provide an information encrypting transmission and reception method in which separate transmission and reception of electronic signature are not required so that a sender and a receiver does not have to disclose their key information to each other, and it is very difficult or substantially impossible for a third person to interpret the key information or the encrypted information while the information is 100% reproducible by the receiver.

SOLVING MEANS

Providing a sender server computer 5 for transmitting and receiving data of a sender 5 and a receiver server computer 6 for transmitting and receiving data of a receiver 4 that are connected to the web network; firstly encrypting bit data FD of original information such as plaintext to be transmitted from the sender 3 to the receiver 4 by performing an exclusive OR operation in use of bit data of electronic key of the sender 3 and transmitting the firstly encrypted bit data CR1 attached with personal data of the receiver 4 to the sender server computer 5; by the sender server computer 5, receiving bit data CS of the electronic key of the receiver 4 by submitting personal data of the receiver 4 to the data center 2, secondly encrypting the firstly encrypted bit data CR1 by performing exclusive OR operation in use of received bit data CS of the electronic key of the receiver 4, and transmitting the secondly encrypted bit data CR2 attached with personal data of the sender 3 and the receiver 4 to the receiver server computer 6; by the receiver server computer 6, receiving the secondly encrypted bit data CR2, receiving bit data BP of the electronic key of the sender 3 by submitting personal data of the sender 3 to the data center 2, thirdly encrypting the secondly encrypted bit data CR2 by performing exclusive OR operation in use of received bit data BP of the electronic key of the sender 3, and informing the receiver 4 about the reception of the thirdly encrypted bit data CR3 or transmitting the thirdly encrypted bit data CR3 to the receiver 4; and by the receiver 4, obtaining the original information such as plaintext from the sender 3 by performing an exclusive OR operation on the thirdly encrypted bit data CR3 in use of the bit data CS of the electronic key of the receiver 4.

Fig. 1