SYSTEM AND METHOD FOR ANTHENTICATION, AND DEVICE AND METHOD FOR AUTHENTICATION

ABSTRACT

In authentication using a plurality of cipher keys, the authentication time is shortened. In the case that an encipher key to encipher key are required to take an access to each area out of the area to area in a memory of an IC card, a plurality of areas to have an access is informed to the IC card from a reader writer, a plurality of cipher keys corresponding to these areas (for example, cipher key 1, cipher key 2, and cipher key 4) is read out, and reduction processing section generates one reduction key from these cipher keys. A random number which is generated from a random number generation section of the reader writer is transferred to the IC card, and an encipherment section enciphers the random number using the reduction key. The reader writer receives the enciphered random number from the IC card, and deciphers it using the reduction key, and judges the IC card to be proper if the deciphered random number is equal to the generated random number.

Figure 2