★★★　＜知的財産翻訳検定＞答案用紙　★★★

==========

科　　目：電気・電子工学

氏　　名：坂本真希

==========

WHAT IS CLAIMED IS:

1.　A cipher communication device comprising

cipher recording means comprising:

error-correction coding means for performing error-correction coding by adding redundancy to inputted data;

interleaving means for rearranging and outputting the data, outputted from the error-correction coding means, every predetermined number of bits according to a predetermined rule; and

encrypting means for encrypting the data outputted from the interleaving means to keep contents of the data outputted from the interleaving means confidential; and

cipher reproduction means comprising:

decrypting means for decrypting the inputted encrypted data to be reproduced by an arbitrary recording medium, the inputted encrypted data being the data outputted from the code recording means;

deinterleaving means for rearranging and outputting the data, outputted from the decrypting means, every predetermined number of bits according to a predetermined rule to restore the data rearranged by the interleaving means; and

error-correction decoding means for correcting the data inputted from the deinterleaving means based on the redundancy added by the error-correction coding means.

2.　The cipher communication device of claim 1, wherein each means in the cipher recording means and each means in the cipher reproduction means are provided with information for operation thereof by key information generating means.

In the cipher reproduction means, the data outputted from the cipher recording means is decrypted by the decrypting means 5. Then, a continuous error in the data outputted from the decrypting means due to an error in the data occurred in the arbitrary recording medium is converted into a pseudo random error by the deinterleaving means 6. This process is shown in Figures 3 (a), 3 (b) and 3 (c). Here, assuming that the encrypting means 3 and the decrypting means 5 handle block cipher, if the data inputted to the decrypting means 5 includes an error produced during

reproduction from the recording medium, as in block Bi shown at 13 in Figure 3 (a), the block having the error during input of the data will have the error continuously. In the matrix memory configuration shown at 14 in Figure 3 (b), if the deinterleaving means 6 writes sequentially in the direction of the column in a row and sequentially proceeds to the next row, and reads sequentially in the direction of the row in a column and sequentially proceeds to the next column, the block Bi including the error is written in the i-th row of the memory of the deinterleaving means 6, and when it is read, the data in the block Bi including the error appears with being dispersed in the i-th bits of the respective columns (Pj,i designated by 16 in Pj designated by 15 in Figure 3 (c)). In this manner, the block having the continuous error in the data outputted from the decrypting means 5 is dispersed by the deinterleaving means 6, and the error in the data outputted from the deinterleaving means 6 is similar to a random error.