★★★　＜知的財産翻訳検定＞答案用紙　★★★

==========

科　　目：電気・電子工学

氏　　名：阿部　慶子

==========

What is claimed is:

1.　A cryptographic communication apparatus comprising:

encryption recording means comprising: error correction encoding means for performing error correction encoding by adding redundancy to input data; interleave means for rearranging output data from the error correction encoding means in accordance with a rule specified in advance for every given number of bits and outputting the same; and encryption means for encrypting output data from the interleave means to conceal a content of the output data from the interleave means; and

encryption reproducing means comprising: decoding means for receiving output data from the encryption recording means reproduced from a given recording medium as input data and canceling the encryption of the input data; deinterleave means for rearranging output data from the decoding means in accordance with a rule specified in advance for every given number of bits and outputting the same to reconstruct the rearrangement of the output data from the decoding means performed by the interleave means; and error correction decoding means for receiving output data from the deinterleave means as input data and correcting erroneous data among the input data based on the redundancy added by the error correction encoding means.

2.　The cryptographic communication apparatus according to claim 1, wherein each of the means of the encryption recording means and each of the means of the encryption reproducing means are given information for operation respectively from a key information generating means.

In the encryption reproducing means, output data from the encryption recording means is decoded by the decoding means 5. Then, sequential errors in output data from the decoding means 5 caused by data errors occurring in the given recording medium are converted to pseudo random errors by the deinterleave means 6. FIGs. 3(a), 3(b) and 3(c) illustrate the manner thereof. Here, assuming that the encryption means 3 and the decoding means 5 are block signals, if an error occurs in the input data to the decoding means 5 during the process of reproduction from the recording medium, errors occur sequentially in a block in which an error has occurred during input, as shown as the Bi block of 13 in FIG. 3(a). If the deinterleave means 6 assumed as one employing a system in which, in a memory configuration by matrix shown as 14 in FIG. 3(b), on the writing side writing is performed in the direction of columns in a row in

succession to proceed to next rows in succession while on the reading side reading is performed in the direction of rows in a column to proceed to next columns in succession, the block Bi in which the error has occurred is written on the row "i" in the memory of the deinterleave means 6, and on the reading side the data of the block Bi in which the error has occurred emerges in a manner in which it is distributed to the i-th bits of the respective columns (Pj, i16 of Pj 15 in FIG. 3(c)). In this way, the block having sequential errors in the output data from the decoding means 5 is distributed by the deinterleave means 6, and the erroneous data are thereby brought into a state close to a random error when output from the interleave means 6.