★★★　＜知的財産翻訳検定＞答案用紙　★★★

==

科　　目：電気・電子工学

氏　　名：杉浦　まゆみ

==

WHAT IS CLAIMED IS:

1. A cipher communication device comprising:

a cipher recording unit including

an error correction encoder for adding a redundancy to input data to perform error correction encoding,

an interleaving device for rearranging output data from the error correction encoder in accordance with a predetermined rule every predetermined fixed bit number for output, and

an encrypting device for encrypting output data from the interleaving device to keep secrecy of contents of the output data from the interleaving device; and

a cipher reproducing unit including

a decrypting device for decrypting input data, the input data being output data from a recording medium recorded by the cipher recording unit,

a de-interleaving device for rearranging output data from the decrypting device in accordance with a predetermined rule every predetermined fixed bit number to restore the order of the output data from the decrypting device, which has been rearranged by the interleaving device, into an original order, and

an error correction decoder for performing correction decoding of an error in input data based on the redundancy added thereto by the error correction encoder, the input data being output data from the de-interleaving device.

2. The cipher communication device according to claim 1, further comprising a key information generator each adapted for the cipher recording unit and the cipher reproducing unit to operate the error correction encoder, the interleaving device, and the encrypting device of the cipher recording unit, and the decrypting device, the de-interleaving device, and the error correction decoder of the cipher reproducing unit.

Upon receiving data from the cipher recording unit, the decrypting device 5 in the cipher reproducing unit is operated to decrypt the encrypted data. After the decryption, the de-interleaving device 6 performs a pseudo random conversion with respect to a consecutive error, which has occurred during reproduction of the data from the recording medium by the decrypting device 5. FIGS. 3A, 3B, and 3C are illustrations showing the operations of the cipher reproducing unit. Assuming that input/output data of the ciphering device 3 and the deciphering device 5 are block ciphers, if an error occurs during reproduction of the data from the recording medium, and the error is included in the output data from the deciphering device 5, as shown in FIG. 3A, Bi block in a data string indicated by the reference numeral 13 carries the error consecutively. In a matrix memory configuration indicated by the reference numeral 14 in FIG. 3B, the de-interleaving device 6 is operated in such a manner that data is sequentially written in a column direction in one row, and the data writing is executed one row after another, and that the data is sequentially read in a row direction in one column, and the data reading is executed one column after another. Under the condition, the block Bi carrying the error is written in the i-th row in the memory of the de-interleaving device 6, and is read in a distributive manner in the i-th bit of each column (see Pj in data string 15, and (Pj, i) in data string 16 in FIG. 3C). In this way, the consecutive error in the block in the output data from the decrypting device 5 is distributed by the de-interleaving device 6, which may be outputted in a pseudo random manner from the de-interleaving device 6.