2005 年第 2 回知的財産翻訳検定

電気電子工学分野標準解答

問題：
下に掲載した課題文中の二つの指定箇所（＊＊＊START＊＊＊から＊＊＊END＊＊＊まで）を翻訳しなさい。なお、二つの翻訳の順序は指定箇所の順序通りとするが、それぞれ米国特許明細書に使用することを前提とした翻訳とすること。

＊＊＊START＊＊＊

【特許請求の範囲】

１．入力データに対して冗長性を付加して誤り訂正符号化を行う誤り訂正符号化手段と、該誤り訂正符号化手段の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するインターリーブ手段と、該インターリーブ手段の出力データの内容を秘匿するために該インターリーブ手段の出力データを暗号化する暗号化手段とを備えた暗号記録手段と、

任意の記録媒体より再生される上記暗号記録手段の出力データを入力データとし、該入力データに対する暗号化を解除する復号化手段と、該復号化手段の出力データの上記インターリーブ手段によるデータの並べ換えを元の順序に復元するために、上記復号化手段の出力データを一定のビット数ごとにあらかじめ指定された規則に従い並べ換えて出力するデインターリーブ手段と、該デインターリーブ手段の出力データを入力データとし、上記誤り訂正符号化手段により付加された冗長性をもとに上記入力データ中の誤ったデータを訂正する誤り訂正復号手段とを備えた暗号再生手段とを備えたことを特徴とする暗号通信装置。

What is claimed is[1]:

1. A cryptography[2] communication apparatus[3], comprising[4]:

cryptography recording means[5] including[6]

error-correction[7] coding[8] means for performing[9] error-correction coding[8] on input data by adding redundancy thereto[10],

interleaving[11] means for arranging[12] data output from[13] the error-correction coding means by sorting[14] every predetermined number[15] of bits in accordance with[16] a predefined[17] rule[18] and outputting the sorted data, and

encrypting[19] means for encrypting[20] the sorted data output from the interleaving means to conceal[21] contents[22] of the sorted data; and

cryptography reproducing[23] means including

decrypting[24] means for receiving[25] as input data the encrypted data output from[26] the cryptography recording means and reproduced from an arbitrary recording medium[27] and decrypting the encrypted data[28],

deinterleaving[29] means for rearranging[29] the data output from the decrypting means by sorting every predetermined number of bits in accordance with a[30] predefined rule in order to restore[31] the original order of the data sorted by the interleaving means, and

error-correction decoding[32] means for receiving as input data the rearranged data output from the deinterleaving means and correcting incorrect[33] data in the input data on the basis of[34] the redundancy added by the error-correction coding means.

[1] We claim, I claim, What we claim is, What I claim is, etc.

[2] cipher (or cypher), cryptographic, encryption,

[3] device, unit, etc.

[4] which comprises

[5] means + function: cryptography recording means; alternatives include: cipher recorder, cipher recording unit/device; cryptography/cryptographic/cipher recording means/unit/device, cryptographic recorder etc. (similarly elsewhere for means + function)

[6] having

[7] error correction

[8] processing

[9] for executing, for carrying out, that performs, that carries out, that executes etc. (similarly elsewhere)

[10] by adding redundancy to input data

[11] arranging, data arranging, sorting, data sorting etc

[12] sorting, ordering

[13] output data of (similarly elsewhere), data outputted from (similarly elsewhere)

[14] arranging

[15] certain, specific, predecided

[16] according to, on the basis of

[17] specific, certain, predetermined

[18] algorithm, formula

[19] enciphering, encyphering, encipherment, encryption, encoding

[20] enciphering, encyphering

[21] hide

[22] content, the content

[23] recovery, reproduction

[24] deciphering, deciphering, decipherment, decryption, decoding

[25] accepting

[26] encrypted output data of, enciphered output data of, output data of, data output from

[27] a recording medium, an arbitrary storage medium, a storage medium

[28] performing/carrying out/executing decryption/deciperment thereof

[29] re-sorting, rearranging

[30] another

[31] recover

[32] processing

[33] false, erroneous

[34] by means of, using, with, utilizing

２．上記暗号記録手段の各手段及び上記暗号再生手段の各手段は、それぞれ鍵情報発生手段により動作のための情報が与えられることを特徴とする特許請求の範囲第１項記載の暗号通信装置。 ＊＊＊END＊＊＊	2. The cryptography communication apparatus according to Claim 1, further comprising: key information[35] generating[36] means for generating[36] key information[37] for each means of[38] the cryptography recording means, and each means of[39] the cryptography reproducing means.

[35] key

[36] producing

[37] a key

[38] for each of the error-correction coding means, the interleaving means, and the encrypting means

[39] each of the decrypting means, the deinterleaving means, and the error-correction decoding means

＊＊＊START＊＊＊ 暗号再生手段においては、上記暗号記録手段からの出力データが復号化手段５により復号される。そして該復号化手段５の出力データ中の上記任意の記録媒体において起こったデータの誤りによる連続的な誤りは、デインターリーブ手段６により擬似的なランダム誤りに変換される。第３図（ａ），（ｂ），（ｃ）はこの様子を示したものである。ここで仮に、暗号化手段３及び復号化手段５がブロック暗号であるとすると、復号化手段５の入力データに、記録媒体より再生される過程で誤りが発生した場合、第３図（ａ）の１３におけるＢｉブロックに示すように、入力中に誤りの発生したブロックは連続的に誤りが発生する。デインターリーブ手段６を、第３図（ｂ）の１４に示す行列によるメモリ構成において、書き込み側は行中の列方向に順次書き込みを行い順次行を進め、読み出し側は列中の行方向に読み出しを行い順次列を進めていく方式のものとすると、上記誤りの発生したブロックＢｉはデインターリーブ手段６のメモリ中の第ｉ行に書き込まれ、読み出し側では上記誤りの発生したブロックＢｉのデータは各列の各々ｉ番目のビットに分散して現われる。（第３図（ｃ）におけるＰｊ１５中のＰｊ,ｉ１６）。このように、復号化手段５の出力データ中の連続的な誤りの存在するブロックは、デインターリーブ手段６により分散され、デインターリーブ手段６の出力では誤ったデータはランダム誤りに近い状態となることとなる。 ＊＊＊END＊＊＊	In the cryptography reproducing means, the decrypting means 5 decrypts the data output from the cryptography recording means[40]. Then, the deinterleaving means 6 converts[41] serial[42] errors that remain[43] in the data decrypted by[44] the decrypting means 5 due to the presence of[45] false[46] data in the encrypted data recorded on the arbitrary recording medium into pseudo-random[47] errors. FIGs. 3A, 3B, and 3C illustrate this process[48]. More specifically[49], assuming that the encrypting means 3 and the decrypting means 5 operate as block cryptography means, when an error occurs[50] in data to be input to[51] the decrypting means 5 during reproduction of the data[52] from the recording medium, the error that occurred during input of the data appears as a serial error in a block Bi in output data 13, as indicated in FIG. 3A. In a memory configuration of a matrix 14[53], as shown in FIG. 3B, the deinterleaving means 6 is configured to sequentially write data[54] in rows[55] on a writing[56] side in a direction of increasing column number[57], proceeding[58] sequentially from row to row[59] in a direction of increasing row number[60], and to sequentially read data[61] from columns[62] on a reading[63] side in a direction of increasing row number, proceeding sequentially from column to column[64] in a direction of increasing column number. The above-described block Bi having the error is written in an ith row of the memory of the deinterleaving means 6 and, on the reading side, the data of the block Bi having the error appears in an ith bit in each of the columns (i.e., Pj,i 16 in Pj 15 shown in FIG. 3C). In this way[65], the block including serial errors generated in the data output from the decrypting means 5 is dispersed by the deinterleaving means so that the errors in the data output from the deinterleaving means 6 are substantially randomized[66].

[40] Passive form: the data output from the cryptography recording means is decrypted by the decrypting means 5

(Similarly throughout)

[41] changes, alters

[42] continuous, consecutive

[43] remaining

[44] the decrypted output data of, the output data of, the (decrypted) data output/outputted from

[45] attributable to, corresponding to

[46] incorrect, erroneous

[47] pseudorandom

[48] operation, conversion process

[49] precisely

[50] in the event of the occurrence of an error

[51] the input data of

[52] when the data is reproduced

[53] In a memory configured to operate in a matrix format, as denoted by reference numeral 14, In a memory having a configuration of a matrix 14, In a memory having a configuration of a matrix, as denoted by reference numeral 14

[54] sequentially writes data, sequentially performs data writing

[55] each row

[56] data writing

[57] an increasing-column-number direction

[58] moving

[59] between rows

[60] an increasing-row-number direction

[61] sequentially reads data, sequentially performs data reading

[62] each column

[63] data reading

[64] between columns

[65] Accordingly, Thus, Thereby

[66] made random