

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 6 部門第 2 区分
 【発行日】平成 24 年 9 月 20 日 (2012.9.20)

【公開番号】特開 2010-72644 (P2010-72644A)
 【公開日】平成 22 年 4 月 2 日 (2010.4.2)
 【年通号数】公開・登録公報 2010-013
 【出願番号】特願 2009-211965 (P2009-211965)
 【国際特許分類】

G 0 9 C 1/00 (2006.01)

【 F I 】

G 0 9 C 1/00 6 5 0 A

【手続補正書】

【提出日】平成 24 年 8 月 6 日 (2012.8.6)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

暗号指数アルゴリズムの指数である第一の正の整数 n を再コード化する正則な方法であって、

当該方法は、プロセッサにおいて、

n よりも小さい第二の整数 s を選択し、

第三の整数 $n' = n - s$ を定義し、

第四の整数 m について、第三の整数 n' の m 変数の表現を桁毎に s の m 変数の表現に加算して、 n の再コード化された表現を生成する、
 ステップを含むことを特徴とする方法。

【請求項 2】

前記 m は、 $m = 2^k$ である、

請求項 2 記載の方法。

【請求項 3】

【数 9】

$$s = \sum_{i=0}^{I-2} s_i m^i$$

であり、前記 I は n の m 変数の長さを示す、
 請求項 1 又は 2 記載の方法。

【請求項 4】

$0 < \alpha < m$ について、 $s_i = \alpha$ である、

請求項 3 記載の方法。

【請求項 5】

$\alpha = 1$ である、

請求項 4 記載の方法。

【請求項 6】

$\alpha = m - 1$ である、

請求項 4 記載の方法。

【請求項 7】

暗号指数アルゴリズムの指数である第一の正の整数 n を正則に再コード化する装置であって、

当該装置はプロセッサを備え、

前記プロセッサは、 n よりも小さい第二の整数 s を選択し、第三の整数 $n' = n - s$ を定義し、第四の整数 m について、第三の整数 n' の m 変数の表現を桁毎に s の m 変数の表現に加算して、 n の再コード化された表現を生成する、ことを特徴とする装置。

【請求項 8】

プロセッサにより実行されたとき、請求項 1 乃至 6 の何れか記載の方法を実行する命令を記憶するコンピュータプログラム。