【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17年6月16日(2005.6.16)

【公表番号】特表2001-510583(P2001-510583A)
【公表日】平成13年7月31日(2001.7.31)
【出願番号】特願平10-526772
【国際特許分類第７版】
　Ｇ０９Ｃ　1/00
【ＦＩ】
　Ｇ０９Ｃ　1/00　６２０Ｂ
　Ｇ０９Ｃ　1/00　６５０Ｚ

【手続補正書】
【提出日】平成16年9月9日(2004.9.9)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】補正の内容のとおり
【補正方法】変更
【補正の内容】

手　続　補　正　書

16.9.-9 適

平成　年　月　日

特許庁長官　小　川　　洋　殿

1.事件の表示　　平成１０年特許願第５２６７７２号

2.補正をする者

事件との関係　出　願　人

名　称　　タンデム　コンピューターズ　インコーポレイテッド

3.代　理　人

住　所　東京都千代田区丸の内３丁目３番１号
電話（代）3211-8741

氏　名　(5995) 弁理士 中　村　　稔

4.補正命令の日付　　自　　発

5.（本補正により請求の範囲に記載された請求項の数は合計「４」となりました。）

6.補正対象書類名　　明細書

7.補正対象項目名　　請求の範囲

8.補正の内容　　別紙記載の通り

特許庁 16.9.10 出願支援室 金井

請求の範囲

１．　暗号通信を設定する方法であって：

プレーンテキストメッセージワードＭを暗号テキストワードＣに暗号化する段階であり、Ｍはメッセージを表す数字に対応しかつ

$$0 \leqq M \leqq n-1$$

であり、ｎは$p_1 \cdot p_2 \cdot \ldots \cdot p_k$の積から形成される合成数、ｋは２より大きい整数であり、$p_1 \cdot p_2 \cdot \ldots \cdot p_k$は個別の素数、及びＣはメッセージワードＭの暗号化した形式を表す数字であり、前記暗号化段階は、前記メッセージワードＭを前記暗号テキストワードＣに変換する段階を具備し、それにより

$$C \equiv M^e \pmod{n}$$

であり、かつｅが$(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)$に対して互いに素である数である、該段階と、

前記暗号テキストワードＣを受け取りメッセージワードＭ´に解読する段階であり、該解読する段階は、

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1))$によって定義される解読指数ｄを用いて実行され、

該解読する段階は、

$$M_1' \equiv C_1^{d1} \pmod{p_1},$$
$$M_2' \equiv C_2^{d2} \pmod{p_2},$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$M_k' \equiv C_k^{dk} \pmod{p_k},$$

ここで、

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$
$$\cdot$$
$$\cdot$$

$C_k \equiv C \pmod{p_k}$

$d_1 \equiv d \pmod{(p_1-1)}$、

$d_2 \equiv d \pmod{(p_2-1)}$、及び

.

.

.

$d_k \equiv d \pmod{(p_k-1)}$、

に従って複数のｋサブータスクを定義する更なる段階と、

結果M_1'、M_2'、...、M_k'を決定するために前記サブータスクを解く更なる段階とを含む、該段階と、及び

M'＝Mである、受け取りメッセージワードM'を生成するために前記サブータスクの前記結果を組み合せる段階とを具備する

ことを特徴とする方法。

２．　前記組み合せる段階は、チャイニーズ剰余定理（ＣＲＴ）の形式を用いることを特徴とする請求項１に記載の方法。

３．　通信を設定するための暗号化通信システムであって：

通信媒体；

前記通信媒体に結合され、転送メッセージワードMを暗号テキストワードCに変換しかつ該媒体に該暗号テキストワードCを転送するように構成された暗号化手段であり、Mはメッセージを表す数字及びｎが

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

という形式の合成数である場合の$0 \leqq M \leqq n-1$に対応しており、ｋは２より大きい整数であり、かつp_1、p_2、...、p_kは個別の素数であり、該暗号テキストワードCは該メッセージワードMの暗号化された形式を表す数字に対応しかつ

$$C \equiv M^e \pmod{n}$$

に対応し、ここでｅが$lcm(p_1-1), (p_2-1), \ldots,$及び$(p_k-1)$に対して互いに素である数であるような、該暗号化手段；及び

前記通信媒体に通信可能に結合され、当該通信媒体を介して前記暗号テキスト

ワードＣを受け取るための解読手段であり、該解読手段は、前記暗号テキストワードＣを受け取りたメッセージワードＭ’に変換するための解読処理を実行するように動作し、Ｍ’は、Ｃの解読された形式を表す数字に対応し、かつ前記解読処理は、

$d \equiv e^{-1} \bmod ((p_1-1)(p_2-1)\ldots(p_k-1))$によって定義される解読指数ｄを用いて実行され、

該解読する段階は、

$M_1' \equiv C_1^{d1} \pmod{p_1}$、

$M_2' \equiv C_2^{d2} \pmod{p_2}$、

.

.

.

$M_k' \equiv C_k^{dk} \pmod{p_k}$、

ここで、

$C_1 \equiv C \pmod{p_1}$、

$C_2 \equiv C \pmod{p_2}$、

.

.

.

$C_k \equiv C \pmod{p_k}$

$d_1 \equiv d \pmod{(p_1-1)}$、

$d_2 \equiv d \pmod{(p_2-1)}$、及び

.

.

.

$d_k \equiv d \pmod{(p_k-1)}$、

に従って複数のｋサブータスクを定義する段階と、

結果M_1'、M_2'、...、M_k'を決定するために前記サブータスクを解く段階とを含み、及び

M’＝Mである、受け取りメッセージワードM’を生成するために前記サブータスクの前記結果を組み合せることを特徴とする暗号化通信システム。

４．　前記複数のｋサブータスクは、並列に実行されることを特徴とする請求項３に記載の暗号化通信システム。