I379572

公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：95105149

※ 申請日期：95.2.21　　※IPC 分類：H04L 9/14 (2006.01)

一、發明名稱：（中文/英文）

用於三階段資料加密之系統與方法

SYSTEM AND METHOD FOR THREE-PHASE DATA ENCRYPTION

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

阿爾塞斯商業集團國際有限公司/ACCESS BUSINESS GROUP INTERNATIONAL LLC

代表人：（中文/英文）

米歇爾　金 S./MITCHELL, KIM S.

住居所或營業所地址：（中文/英文）

美國密西根州亞達城東法爾頓路 7575 號

7575 Fulton Street East, Ada, MI 49355, USA

國　籍：（中文/英文）

美國/U.S.A.

三、發明人：（共 3 人）

姓　名：（中文/英文）

1. 維許　尼馬/VEISEH, NIMA
2. 巴曼　大衛　W./BAARMAN, DAVID W.
3. 里屏　湯瑪斯　J./LEPPIEN, THOMAS JAY

國　籍：（中文/英文）

1. 美國/U.S.A.
2. 美國/U.S.A.
3. 美國/U.S.A.

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國、　2005/2/24、　11/064,912

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係有關於用於三階段資料加密之系統與方法。

【先前技術】

發明背景

隨著通訊網路的激增，且特別係全部或部分透過無線媒體而實作的通訊網路的激增，資料安全性的重要性日益增高。無線網路技術比起有線網路技術相對新。如此，目前安全化無線網路技術係從對有線網路所發展且使用的技術導出。舉例言之，一種安全化網路的技術，無論為有線或無線係將通訊加密。如此防止當網路受損時通訊的內容被未經授權方所理解。目前的加密技術可滿意地用於直接有線網路路徑，並不包括中間的無線部分。為了損害加密傳輸，攻擊者典型必須收聽多次異動，俾便破解加密演繹法則。舉例言之，外側該方為了接取透過直接纜線連接的異動，外側該方可能接取耦接的導線或伺服器，密切監視資料流，直到外側該方判定何時一次異動由伺服器所接收或傳輸為止。另外，外側該方可能試圖存取含於伺服器的資料，諸如儲存於其上的任何安全資料庫。一旦被存取，且收集足夠資料時，攻擊者可將資料解密。已知一些技術可保護儲存於伺服器的資料，有線媒體的相對不容易接取，造成接取與截取有線通訊相當困難。但當通訊係透過無線發射時，攜帶有通訊的無線信號經常係全向廣播，因而於該範圍內可由小心收聽的任何人所接取。如此，實作

來保護伺服器的異動、或透過通訊媒體的異動避開攻擊的技術極少可能保護至少部分透過無線網路行進的異動，透過無線網路，資料無法藉伺服器保護，無線信號無法安全地約束。當異動至少部分透過無線網路行進時，任何人皆可能試圖截取資料流。如此增加一給定的加密演繹法則可能受到攻擊者破壞的機率。

於任何使用無線網路異動時，主要的擔憂之一為外側該方可能可截取異動且解密異動，該異動曾經被加密供保護之用，當解密時外側該方獲得個人資訊及/或安全資訊諸如信用卡卡號、銀行帳號、及社會安全號碼(身分證字號)。因此期望保護無線異動，來防止外側該方截取異動與解密異動。

【發明內容】

本發明係為一種加密一訊息之方法，包含：以已知加密鑰E、第一私密質數P、和第二私密質數Q之函數，來將訊息內容從一第一形式M轉換成為一第二形式M'；根據間隔型樣來將訊息內容分開；以及根據亂序型樣來將訊息內容亂序。

圖式簡單說明

第1圖為根據本發明的一個實施例，一種三階段加密與解密技術之流程圖。

第2圖為該三階段加密技術之轉換階段之一個實施例之流程圖；

第3a圖為該三階段加密技術之分開階段之一個實施例

之流程圖；

第3b圖為第3a圖之三階段加密技術之該實施例之亂序階段之流程圖；

第4a圖為該三階段加密技術之分開階段之另一個實施例之流程圖；

第4b圖為第4a圖之三階段加密技術之該實施例之亂序階段之流程圖；

第5圖為第3a圖和第3b圖之三階段加密技術之該實施例之三階段解密技術之流程圖；

第6圖為第4a圖和第4b圖之三階段加密技術之該實施例之三階段解密技術之流程圖。

第7圖為加密模組之一個實施例和解密模組之一個實施例之方塊圖；

第8a圖為三階段加密技術之實施例之一個實例之流程圖；

第8b圖為第8a之該實施例之三階段加密技術之一個實施之流程圖；以及

第9圖為有以額外第四階段之三階段加密技術之一個實施例之一個實例之流程圖。

【實施方式】

較佳實施例之詳細說明

第1圖為流程圖100，顯示三階段加密技術之一個實施例和三階段解密技術之一個實施例。須瞭解任何單一元件皆可實作三階段加密技術、三階段解密技術或其組合。

一般而言，所揭示之三階段加密和解密技術可用來保護至少部分透過無線網路進行的通訊。但熟諳技藝人士瞭解所揭示的三階段加密和解密技術可用來透過有線媒體或任何其它型別的通訊媒體通訊。

三階段加密技術通常係由發射元件用來於發射訊息至接收元件前加密訊息。發射元件加密該訊息，防止外側該方容易截取通過通訊媒體而行進至接收的元件訊息，且防止外側該方存取諸如信用卡卡號、銀行帳號和身分證字號等個人資訊及/或安全資訊。

三階段解密技術通常係由接收元件用來於接收到來自於發射元件的訊息後，接收元件解密該訊息。接收元件解密該訊息來存取三階段加密技術所保護的諸如信用卡卡號、銀行帳號和身分證字號等個人資訊及/或安全資訊。

於一個實施例中，具有加密能力的發送/發射元件使用所揭示的三階段加密技術102加密訊息，且發送該訊息至接收元件110。須瞭解此種通訊可為雙向，多種元件皆可從事發送與接收二者。如此，此處使用的發送元件或接收元件的分配指示一種構想上的應用，一次通訊的發送元件也可是另一次通訊的接收元件等。發送元件可包括個人電腦；個人數位處理器；伺服器；工作站；家電例如智慧型家電諸如洗衣機/乾衣機、冰箱、淨水系統或烤爐其可操作來透過網路發送或接收資料；或任何其它型別技藝界已知之可於網路運作的元件、或其組合、包括非網路可運作的元件經式樣翻新或以其它方式調整適應變成網路可運作。接收

元件接收訊息111，使用所揭示的三階段解密技術112來解密加密的訊息。類似加密元件，接收元件可包括個人電腦；個人數位處理器；伺服器；工作站；家電例如智慧型家電諸如洗衣機/乾衣機、冰箱、淨水系統或烤爐其可操作來透過網路發送或接收資料；或任何其它型別技藝界已知之可於網路運作的元件、或其組合、包括非網路可運作的元件經式樣翻新或以其它方式調整適應變成網路可運作。

用來從加密元件發送加密的訊息110至接收元件的無線協定可包括與IEEE 802.11標準集合諸如802.11(a)、802.11(b)、或802.11(g)可相容的無線保真度(「Wi-Fi」)；通用封包無線服務(「GPRS」)；藍芽、衛星發射或蜂巢式發射；超寬頻；WiMax；或任何其它型別之使用射頻(RF)、光或其它傳輸媒體的無線協定，且可進一步包括透過網路各部分的不同無線技術的組合。

於欲透過網路發射之訊息操作三階段加密技術102時，訊息內容從第一形式M轉換成為第二形式M'104，典型係使用質因數分解來轉換，來於傳輸期間隱藏訊息的原始內容。

然後將訊息內容分開106，典型係分開成為多個分開的封包或多個分開組群，容後詳述，來將訊息內容發射的時間間隔解除均勻化，藉此來增加第三方收聽傳輸，解密訊息內容的困難。

於一個實施例中，為了分開訊息的內容，可分解訊息的內容，讓部分訊息內容展開於多個分開的封包內，各個

封包於發射時係以給定的時間量分開。於另一個實施例中，為了分開訊息內容，過量符號諸如空間插入訊息內容，來將訊息內容分配於多個組群。

最後，含有訊息內容的多個分開封包或多個組群係根據使用者定義的型樣108亂序，其實例容後詳述。

欲解密已經使用前述三階段加密技術102所加密的訊息，三階段加密技術102單純被逆轉112。典型地為了提高安全度，接收元件將知曉解密一個已經使用所揭示的三階段加密技術102加密的訊息所需的演繹法則和變數。但於其它實施例中，所需解密訊息的演繹法則和變數可進送於接收元件，但安全度降低。

最初，經由逆轉使用者定義的型樣，將多個分開脈衝或多個群組內部的訊息內容整序114。其次，包含訊息內容的多個封包被重整返回單一訊息，或於多個群組間的過量符號被去除116，採用之方式係依據用來分解原先訊息的方法決定。典型地，用來分解原先訊息的方法係以一位數或二位數的形式指示於訊息的標頭。最後，訊息內容從第二形式M'被轉換成為第一形式M 118。

第2圖為流程圖，顯示該三階段加密技術之轉換階段200之一個實施例。典型地，於訊息內容的字母順序語法被轉換成為數值表示型態202。舉例言之，字母「a」可轉換成以數值表示為01，字母「b」可轉換成以數值表示為02等等。字母的轉換可遵照資訊交換之美國標準碼(「ASCII」)或擴充二進制碼十進制互換碼(「EBCDIC」)標準或可為任

意轉換。將字母語法轉換成為數值表示形態的功能為眾所周知，大部分的程式語言皆包括執行此項運算型別的標準功能。

為了將訊息內容從第一形式M轉換成第二形式M'，進送元件及/或接收元件的加密構件和解密構件係以第一私密質數P、第二私密質數Q、已知加密鑰E和私密加密鑰D程式規劃。此外，第一私密質數和第二私密質數之積定義為N。

為了提高安全性，已知加密鑰須相對於第一私密質數P和第二私密質數Q為互質206因此：

$$GCD(E,(P-1)^*(Q-1))=1$$

其中GCD為最大通用除數或因數。如眾所周知，兩個或更多整數若除了數目1之外並未共享共通的正因數(除數)，則可被定義為互質。

私密解密鑰D典型並非公開已知。私密解密鑰D用來解密由接收元件所接收到的任何訊息。於選擇第一私密質數P、第二私密質數Q、及已知加密鑰E之後，私密加密鑰D可使用下式求出：

$$D^*E=1^*\mathrm{mod}((P-1)^*(Q-1))。$$

使用第一私密質數P與第二私密質數Q的積N，以及使用已知加密鑰E，訊息內容從第一形式M根據下式被轉換208成為第二形式M'：

$$M'=M^E\mathrm{mod}N。$$

注意為了讓從第一形式M轉換208成為第二形式M'可正確運作，N的數值須大於第一形式M中訊息內容之數值。

第3a圖和第4a圖為三階段加密技術的分開階段之流程圖。典型地，訊息內容係於轉換階段之後分開，但於其它實施例中，訊息內容可於轉換期之前分開。

於第3a圖所示的一個實施例中，為了分開訊息內容，訊息內容經過分解300，讓訊息內容展開於多個分開的封包304。典型地，為了決定多個分開封包的間隔型樣，選用第三私密質數R和第二已知加密鑰K。公開已知之加密鑰K之數值可為任何模數，諸如10、私密加密鑰D之數值或任何其它推薦值。

於一實施例中，間隔型樣可為於多個分開封包間加密元件所等候的多個符號。但於其它實施例中，使用者可選擇讓間隔型樣之數值係與就多個分開封包間的間隔相關的其它定義相對應。間隔型樣典型係根據下式計算302：

$$F(R)=R^{*}\bmod(K)。$$

於若干實施例中，間隔型樣可於「R mod K」與「K—R mod K」間切換或為使用者所選用的任何公式。

於第4a圖所示的另一個實施例中，為了分開訊息內容400，訊息內容之分開方式，係讓過量符號插入於訊息內容404，來將訊息內容分配成為多個組群。過量符號可為空白、或使用者所期望的任何型別的符號。過量符號的間隔型樣可根據前文說明之用來測定第3a圖之實施例之間隔型樣的相同方法測定，典型地，選用第三私密質數R和第二已知加密鑰K。第二已知加密鑰K之數值可為任何模數諸如10、私密加密鑰D之數值、或任何其它推薦之數值。間隔型

樣可根據下式計算402：

$$F(R)=R^{*}\bmod(K)。$$

於若干實施例中，間隔型樣可於「R mod K」與「K—R mod K」間交替，或為使用者所選用的任何公式。

典型地，於間隔階段300、400後，留下的訊息內容區段經亂序306、406。但於其它實施例中，三階段加密技術順序可改變，因此於間隔階段300、400或轉換階段200之前，訊息內容被亂序306、406。

第3b圖為第3a圖之實施例之三階段資料加密方法之亂序階段306之流程圖。典型地，選用第四質數S和私密模數J。私密模數J之數值可為任何整數，諸如10、私密加密鑰之一、或一個私密整數集合。第四質數S和私密模數J係用來根據下式計算308亂序型樣：

$$G(S)=S^{*}\bmod(J)。$$

於一個實施例中，亂序型樣表示多個分開封包中的哪一個將根據預先界定的方法亂序。舉例言之，若亂序型樣係等於數目2，則可表示與每隔一個分開封包進行亂序動作。亂序動作包括顛倒兩個數值符號、加上一個常數至數值訊息值、或任何其它使用者所期望的功能310。

第4b圖為第4a圖之實施例之亂序階段406之流程圖。如前文對第3a圖和第3b圖之實施例所述，選用第四質數S和私密模數J。第四質數S和私密模數J用來根據下式計算408亂序型樣：

$$G(S)=S^{*}\bmod(J)。$$

第5圖為根據第3a圖和第3b圖的實施例所形成之加密訊息之解密500之流程圖。於加密元件已經經由三階段加密技術處理訊息後，加密訊息可送至接收元件502。接收元件一旦接收時，逆轉三階段加密技術來解密加密的訊息。

典型地，於多個分開封包內部的訊息內容係單純藉逆轉前文於第3b圖說明之程序而被整序504。典型地，接收元件將已知私密模數J和第四質數S，因而可計算亂序型樣，且剖析訊息的加密內容來逆轉亂序504。

於整序階段504後，包含訊息的多個分開封包重整為單一訊息506。典型地，接收元件將已知第三私密質數R、和第二已知加密鑰K，故接收元件可計算間隔型樣且剖析訊息，來逆轉第3a圖所述之506以上的處理程序。

於多個分開封包被重整為單一訊息506後，訊息內容從第二形式M' 被轉換成第一形式M 510。典型地，接收元件將知曉公開已知之加密鑰E和第一和第二私密質數P、Q。使用E、P和Q，接收元件使用下式來計算508私密解密鑰D：

$$D^*E=1^*\mathrm{mod}((P-1)^*(Q-1))。$$

然後接收元件根據下式，將訊息內容從第二形式M'轉換510成為第一形式M：

$$M=(M')^{D^*}\mathrm{mod}(P^*Q)。$$

第6圖為根據第4a圖和第4b圖之實施例，接收自加密元件602之加密訊息的解密600之流程圖。典型地，藉過量符號所分散的訊息內容係藉單純逆轉前文於第4b圖所述之處理程序而整序604。典型地，接收元件將知曉私密模數J和

第四質數S，可計算亂序型樣且剖析訊息來逆轉亂序程序。

於整序階段604後，包含訊息的多個分開封包被重整606回單一訊息。典型地，接收元件將知曉質數R和第二已知加密鑰K，來計算間隔型樣且剖析訊息，來逆轉前文於第4a圖所述之分開程序。

於多個分開封包被重整606為單一訊息後，訊息內容從第二形式M'被轉換610成為第一形式M。典型地，接收元件將知曉已知加密鑰E、第一私密質數P和第二私密質數Q。使用E、P和Q，接收元件使用下式計算608私密解密鑰D：

$$D^{*}E=1^{*}\mathrm{mod}((P-1)^{*}(Q-1))。$$

然後接收元件根據下式，將訊息內容從第二形式M'轉換610成為第一形式M：

$$M=(M')^{D^{*}}\mathrm{mod}(P^{*}Q)。$$

如同加密程序的各階段順序，於其它實施例中，可顛倒解密程序的各階段順序。

第7圖為方塊圖，顯示使用三階段加密技術來加密訊息之加密模組702之一個實施例、和使用三階段解密技術來解密訊息之解密模組704之一個實施例。加密模組702和解密模組704可為可進行三階段加密技術和三階段解密技術的任何型別的硬體或軟體。單一元件可包含加密模組702和解密模組704二者，故單一元件可進行雙向通訊，或單一元件可包含加密模組702或解密模組704，讓單一元件只可於一個方向通訊。

加密模組702典型包括一加密處理器706、耦接加密處

理器706之一加密記憶體708、以及耦接加密處理器706、加密記憶體708、和通訊網路712之加密網路介面710。此處「耦接」一詞定義為表示直接連接，或透過一個或多個中間構件而間接連接。此種中間構件包括基於硬體和基於軟體之構件。

加密處理器706可為標準奔騰(Pentium)處理器、英特爾(Intel)嵌入型處理器、客端處理器；或任何其它型別之有線處理器，或可執行軟體程式來執行前文說明之將訊息內容從第一型式M轉換成為第二形式M'、根據間隔型樣而分開訊息內容、以及根據亂序型樣來亂序訊息內容等前述功能。典型地，此等功能將呈邏輯以軟體程式實作，儲存於加密記憶體708，且可由加密處理器706所執行。

加密記憶體708可為任一型記憶體諸如ROM或快閃記憶體，或加密記憶體708可為任一型持久性或活動性碟片或驅動器。加密網路介面710可為任一型可透過無線網路、有線通訊網路、或任何其它型別的通訊媒體進行通訊的任一型網路介面。

同理，解密模組704典型包括一解密處理器714、耦接解密處理器714之一解密記憶體716、以及耦接解密處理器714、解密記憶體716及通訊網路712之解密網路介面718。

解密處理器714可為標準奔騰(Pentium)處理器、英特爾(Intel)嵌入型處理器、客端處理器；或任何其它型別之有線處理器，或可執行軟體程式來執行前文說明之將訊息內容從第一型式M轉換成為第二形式M'、根據間隔型樣而分開

訊息內容、以及根據亂序型樣來將訊息內容整序、根據間隔型樣來統一分開的訊息內容、以及將訊息內容形式從第二形式M'轉換成第一形式M等前述功能。典型地，此等功能將呈邏輯以軟體程式實作，儲存於解密記憶體716且由加密處理器714所執行。解密記憶體716可為諸如ROM或快閃記憶體等任一型記憶體，或可為任何型別的持久性或活動性碟片或驅動器。

解密記憶體716可為任一型記憶體諸如ROM或快閃記憶體，或解密網路介面718可為任一型持久性或活動性碟片或驅動器。加密網路介面710可為任一型可透過無線網路、有線通訊網路、或任何其它型別的通訊媒體進行通訊的任一型網路介面。

第8a圖和第8b圖為使用三階段資料加密方法的一個實施例，訊息加密(第8a圖)以及然後解密(第8b圖)之一個實例之流程圖。如第8a圖可知，第一形式M之訊息定義為具有數值23 802。此外，第一私密質數定義為具有數值5，第二私密質數定義為具有數值7，及已知第二加密鑰E定義為具有數值29。如前文說明，第一和第二私密質數之數值為質數，而已知加密鑰E係與該第一和第二私密值數互質。此外，第一和第二質數之積算出為35，滿足第一和第二質數之積須大於第一形式M中之訊息數值的要求。

訊息根據下式，如前文說明，從第一形式M轉換804成為第二形式M'：

$$M'=M^{E*} \bmod (P^{*}Q)$$

$$M'=(23)^{29*}\text{mod}(35)。$$

當執行轉換階段804時，於第一形式M之訊息值23計算於第二形式M'中具有數值18。

於轉換階段804後，執行間隔階段806。於該實例中，第三私密質數定義為31，而第二已知加密鑰定義為10。間隔型樣係根據下式，如前文說明計算806：

$$F(R)=R^{*}\text{mod}(K)$$

$$F(31)=31^{*}\text{mod}(10)，$$

結果獲得數值1。該實例中，數值1定義為單一空格「00」。

於一個實施例中，訊息被分開成為分開的封包808，數值1結果導致訊息從「18」分開成為數值「1__8」，於分開封包間有個單一空格。另外，於一個實施例中，過量空間置於多群間來分散訊息810，訊息從「18」被分離成為有兩個過量符號定義成為一個空格於多群間的數值「1008」。

於間隔階段806後，計算亂序型樣812。於該實例中，第四質數定義為17，私密模數定義為15。亂序型樣係根據下式計算：

$$G(S)=S^{*}\text{mod}(J)$$

$$G(17)=17^{*}\text{mod}(15)，$$

結果獲得數值2。於該實例中，數值2定義為表示每隔一個封包或每隔一群被亂序。

於該實例中，當一群或一個封包被亂序時，定義為表示將常數10加至該數值，且將兩個數值符號顛倒。於一個

實施例中，訊息被分開成為分開的封包808，「1__8」之訊息首先被改成「1__18」然後被改成「1__81」。因此訊息值23具有加密值「1__81」。

於一個實施例中，過量空格置於二群間來分散訊息810，訊息「1008」首先被改成「10018」，然後被改成「10081」。因此訊息值23具有加密值10081。

然後加密元件將加密值10081送至接收元件814。參考第8b圖，接收元件接收此加密訊息818，可首先整序訊息內容820。接收元件必須知曉被亂序的各群或各封包必須有兩個數值符號顛倒且加入數值10至原先訊息。此外，接收元件必須知曉第四質數被定義為17，私密模數被定義為15，因此接收元件可如前文說明正確求出亂序型樣值為2。

於一個實施例中，訊息被分開成為分開封包822，訊息「1__81」首先被改成「1__18」，然後被改成「1__8」820。於一個實施例中，過量空格放置於多群間來分散訊息824，訊息「10081」首先被改成「10018」，然後被改成「1008」820。

於整序階段820後，接收元件將訊息置回同一訊息826。接收元件必須知曉第三私密質數定義為31，公開已知模數定義為10，故接收元件可正確計算間隔型樣為1，且知曉一個空格或「00」被插入於訊息內容的二群或二封包間。

於一個實施例中，訊息被分開成為分開封包822，訊息「1__8」被改成「18」。此外，於一個實施例中，過量空間置於多群間來分散訊息824，訊息「1008」被改成「18」。

最後，接收元件執行轉換階段830，來將訊息內容從第二形式M'轉換回第二形式M。接收元件必須知曉第一私密質數定義為具有數值5，第二私密質數定義為具有數值7，以及已知加密鑰E定義為具有數值29。使用此等值，接收元件根據下式，如前文說明計算828私密解密鑰D：

$$D^{*}E=1^{*}\mathrm{mod}((P-1)^{*}(Q-1))$$

$$D^{*}29=1^{*}\mathrm{mod}(4^{*}6)，$$

結果獲得數值5。使用私密解密鑰D，接收元件根據下式將第二形式M'之訊息轉換830成為第一形式M：

$$M=(M')^{D^{*}}\mathrm{mod}(P^{*}Q)$$

$$M=(18)^{5^{*}}\mathrm{mod}(7^{*}5).$$

上式可獲得830於第一形式M之訊息數值為23，此數值係於執行三階段加密處理前，於第一形式中之訊息值相同。

實作三階段加密技術或三階段解密技術之元件也可將額外階段整合成為三階段加密技術或三階段解密技術。例如如第9圖所示，於一個實施例中，實作第8A圖之三階段解密技術之元件可執行第四階段916，亂序多個封包的順序或多群的順序。如此，只要新階段不會將資料失真至新階段無法被正確逆轉的程度，則任何額外階段皆可增加至三階段加密技術或三階段解密技術。

因此意圖前文詳細說明為說明性而非限制性，須瞭解於後文申請專利範圍包括全部相當例皆意圖界定本發明之精隨及範圍。

【圖式簡單說明】

第1圖為根據本發明的一個實施例，一種三階段加密與解密技術之流程圖。

第2圖為該三階段加密技術之轉換階段之一個實施例之流程圖；

第3a圖為該三階段加密技術之分開階段之一個實施例之流程圖；

第3b圖為第3a圖之三階段加密技術之該實施例之亂序階段之流程圖；

第4a圖為該三階段加密技術之分開階段之另一個實施例之流程圖；

第4b圖為第4a圖之三階段加密技術之該實施例之亂序階段之流程圖；

第5圖為第3a圖和第3b圖之三階段加密技術之該實施例之三階段解密技術之流程圖；

第6圖為第4a圖和第4b圖之三階段加密技術之該實施例之三階段解密技術之流程圖。

第7圖為加密模組之一個實施例和解密模組之一個實施例之方塊圖；

第8a圖為三階段加密技術之實施例之一個實例之流程圖；

第8b圖為第8a之該實施例之三階段加密技術之一個實施之流程圖；以及

第9圖為有以額外第四階段之三階段加密技術之一個實施例之一個實例之流程圖。

【主要元件符號說明】

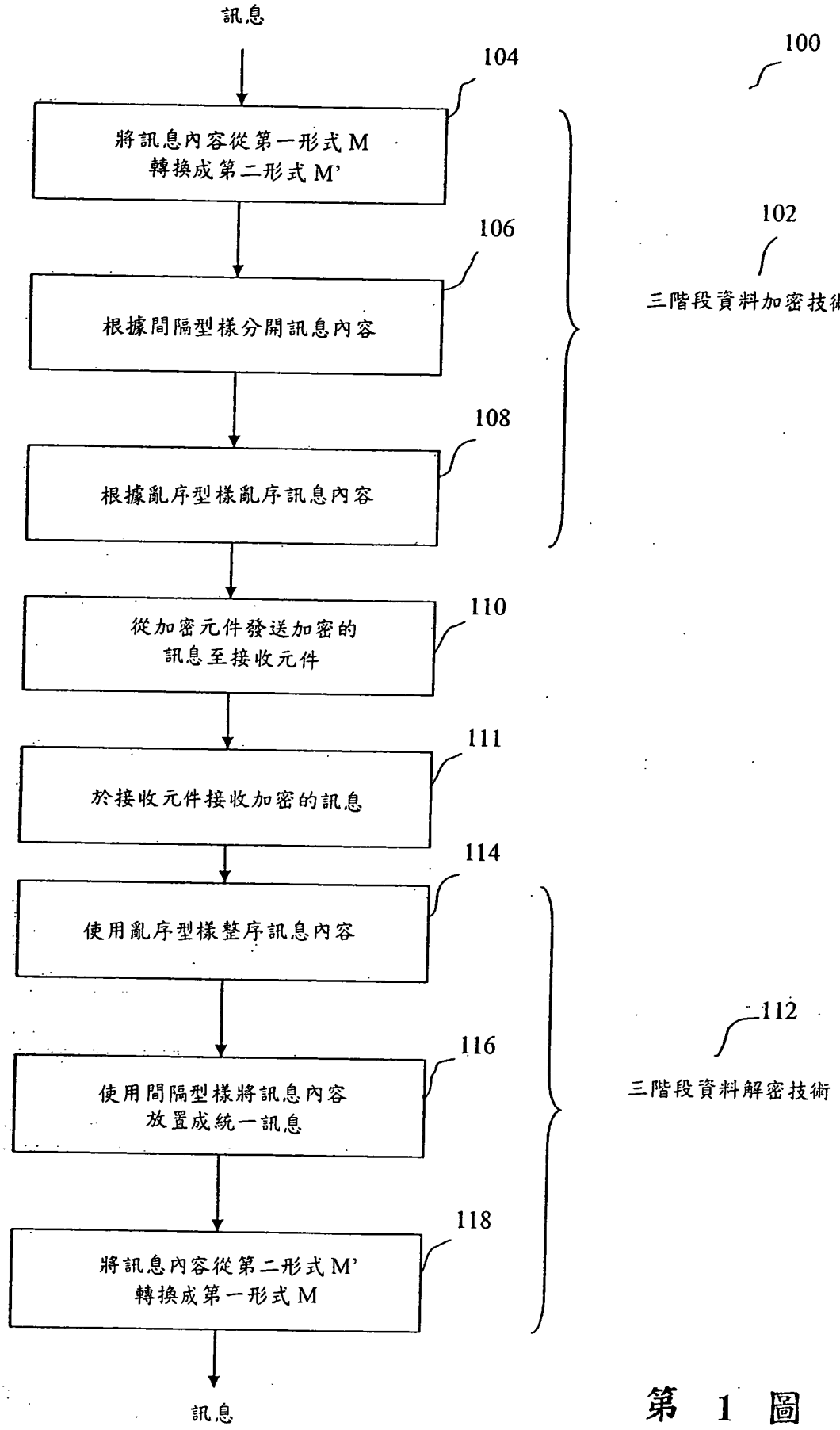
100...流程圖
102...三階段資料加密技術
104-111...動作方塊
112...三階段資料解密技術
114-118...動作方塊
200...流程圖
202-208...動作方塊
300...流程圖
302-304...動作方塊
306...流程圖
308-310...動作方塊
400...流程圖
402-404...動作方塊
406...流程圖
408-410...動作方塊
500...流程圖
502-512...動作方塊
600...流程圖
602-612...動作方塊
702...加密模組
704...解密模組
706...加密處理器
708...加密記憶體
710...加密網路介面
712...通訊網路
714...解密處理器
716...解密記憶體
718...解密網路介面
800...流程圖
802...動作方塊
804...轉換階段
806...間隔階段
808-814...動作方塊
816...流程圖
818...接收階段
820...整序階段
822-828...動作方塊
830...轉換階段

五、中文發明摘要：

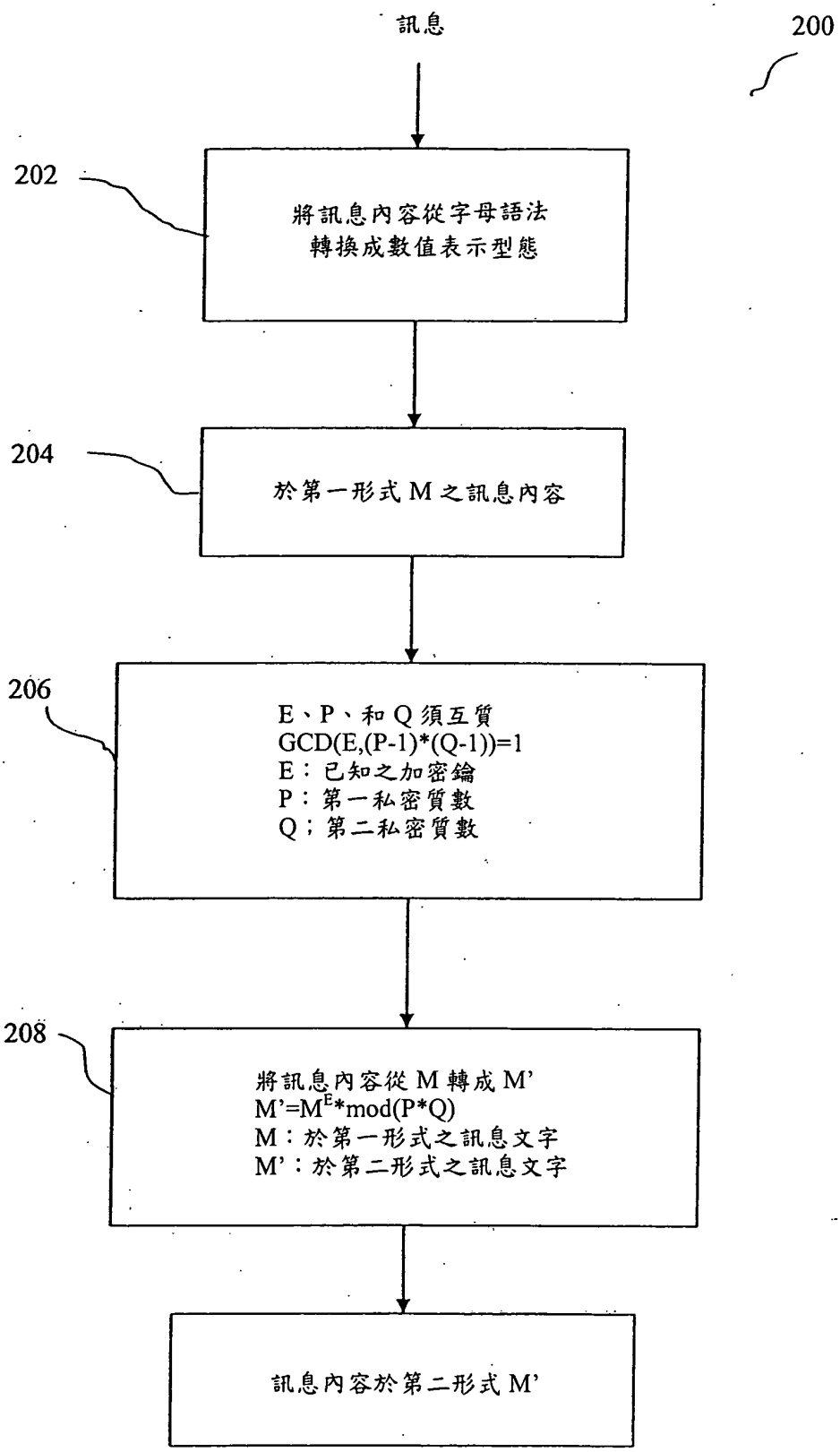
本發明係有關一種三階段加密方法和一種三階段解密方法，以及一種實作該三階段加密方法及/或三階段解密方法之裝置。為了根據三階段加密方法加密訊息，第一形式M轉換成第二形式M'；訊息內容係根據間隔型樣而被分開；以及該訊息內容根據亂序型樣而被亂序，為了使用三階段解密方法來解密加密的訊息，亂序型樣和間隔型樣被逆轉，訊息內容從第二形式M'被轉換成第一形式M。

六、英文發明摘要：

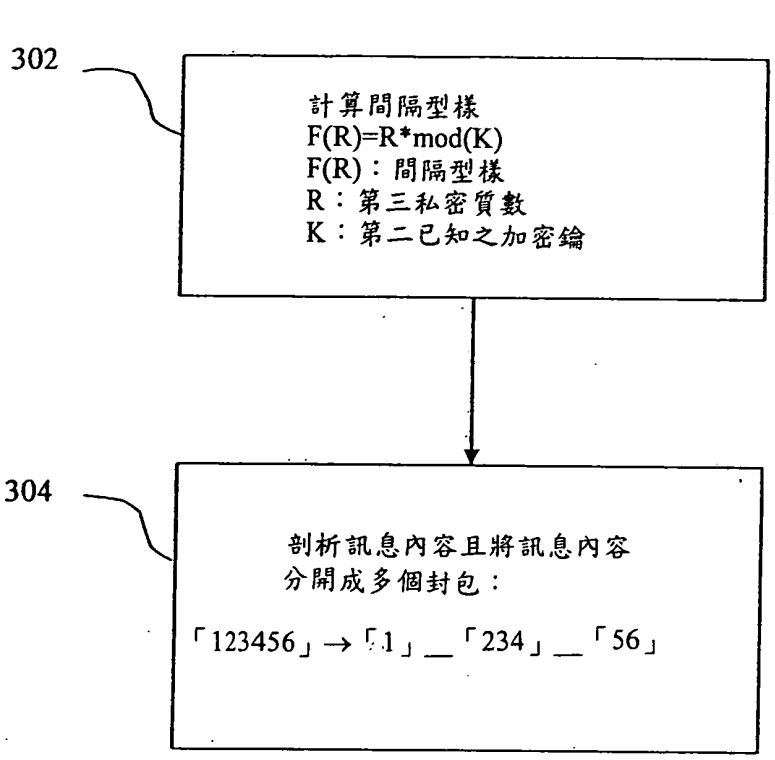
The present invention is directed to a three-phase encryption method and a three-phase decryption method, and an apparatus implementing the three-phase encryption method and/or the three-phase decryption method. To encrypt a message according to the three-phase encryption method, a content of a message is converted from a first form M to a second form M'; the content of the message is separated according to a spacing pattern; and the content of the message is scrambled according to a scrambling pattern. To decrypt the message encrypted using the three-phase encryption method, the scrambling and spacing patterns are reversed, and the content of the message is converted from the second form M' to the first form M.


訊息
100
104
將訊息內容從第一形式 M
轉換成第二形式 M'
102
106
根據間隔型樣分開訊息內容
三階段資料加密技術
108
根據亂序型樣亂序訊息內容
110
從加密元件發送加密的
訊息至接收元件
111
於接收元件接收加密的訊息
114
使用亂序型樣整序訊息內容
112
116
使用間隔型樣將訊息內容
放置成統一訊息
三階段資料解密技術
118
將訊息內容從第二形式 M'
轉換成第一形式 M
訊息

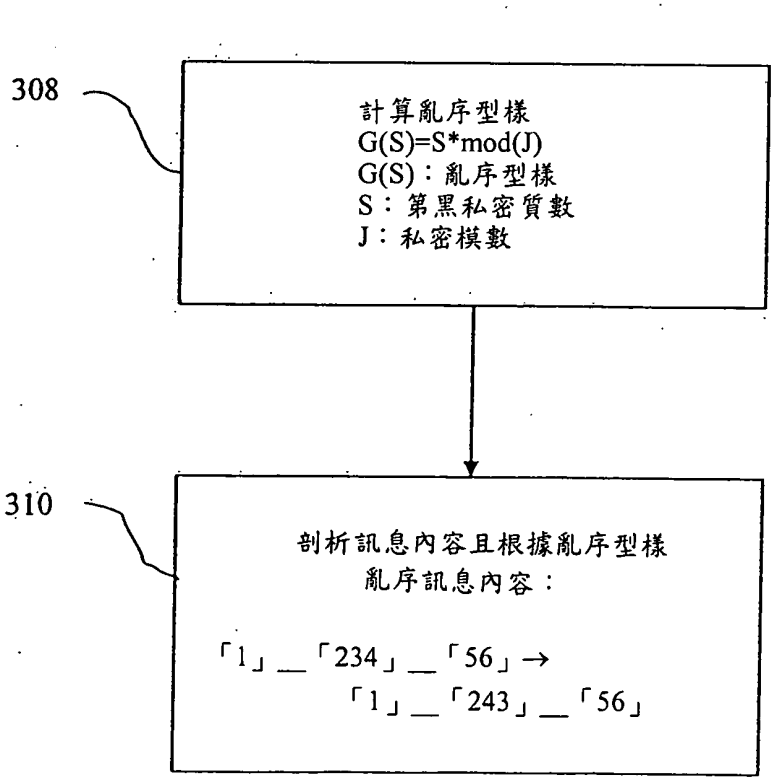
第 1 圖


訊息
200
202
將訊息內容從字母語法
轉換成數值表示型態
204
於第一形式 M 之訊息內容
206
E、P、和 Q 須互質
GCD(E,(P-1)*(Q-1))=1
E：已知之加密鑰
P：第一私密質數
Q；第二私密質數
208
將訊息內容從 M 轉成 M'
M'=M^E*mod(P*Q)
M：於第一形式之訊息文字
M'：於第二形式之訊息文字
訊息內容於第二形式 M'

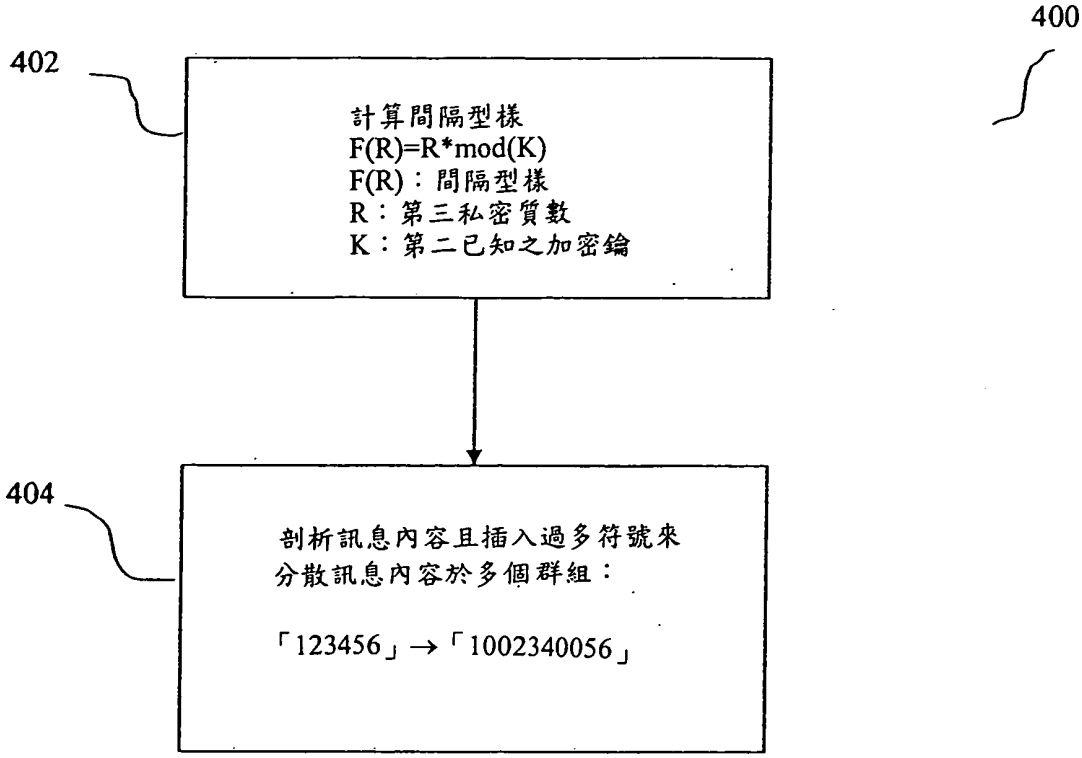
第 2 圖


300
302
計算間隔型樣
F(R)=R*mod(K)
F(R)：間隔型樣
R：第三私密質數
K：第二已知之加密鑰
304
剖析訊息內容且將訊息內容
分開成多個封包：
「123456」→「1」__「234」__「56」

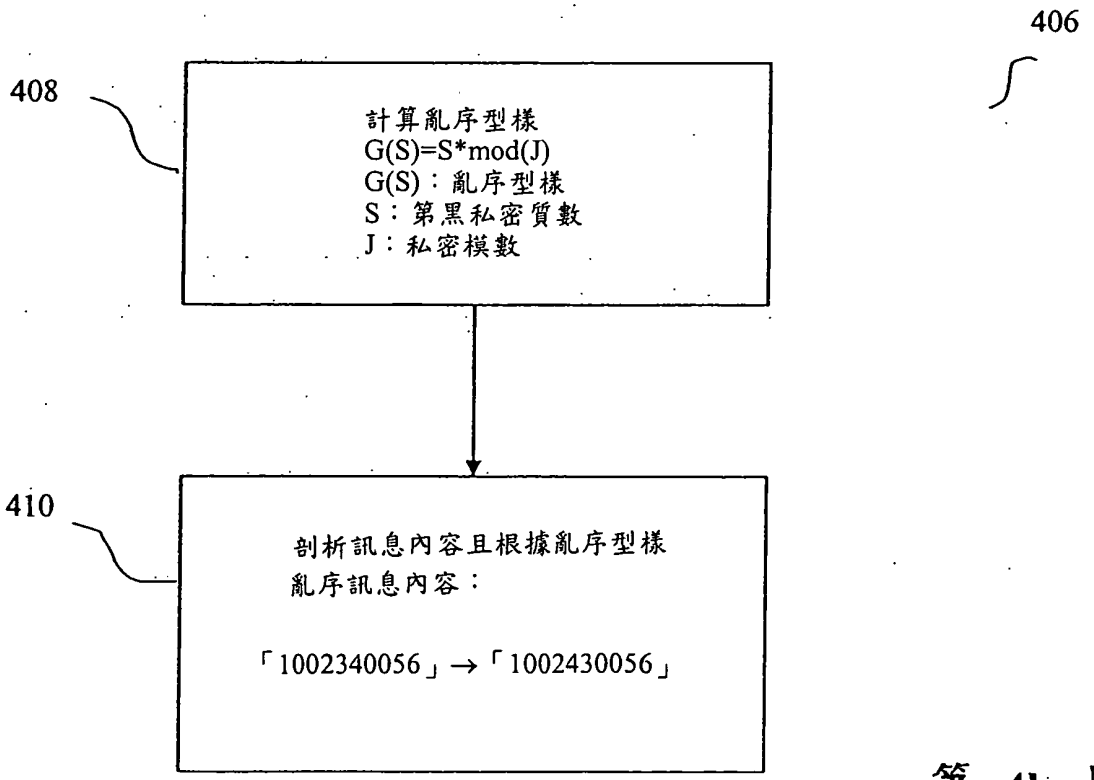
第 3a 圖


306
308
計算亂序型樣
G(S)=S*mod(J)
G(S)：亂序型樣
S：第黑私密質數
J：私密模數
310
剖析訊息內容且根據亂序型樣
亂序訊息內容：
「1」__「234」__「56」→
「1」__「243」__「56」

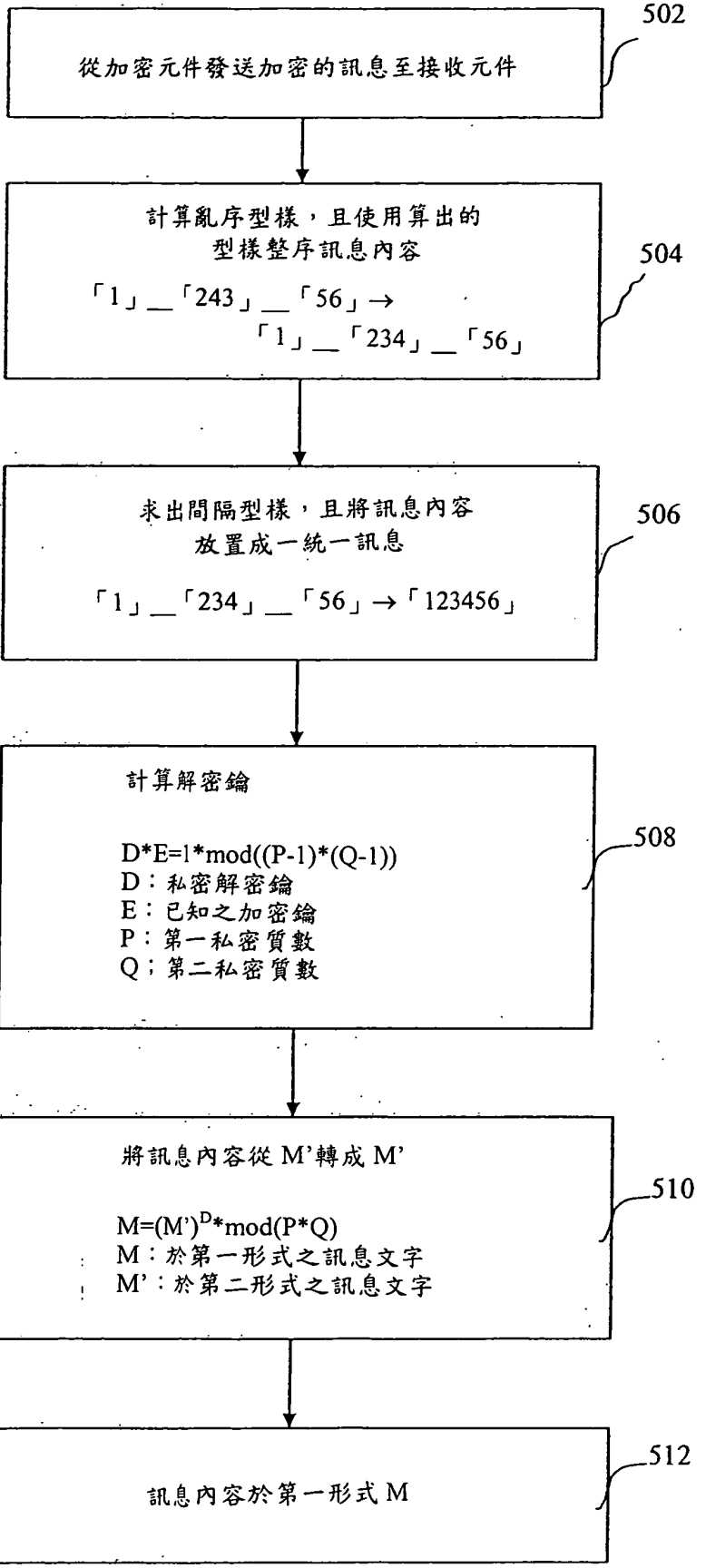
第 3b 圖


400
402
計算間隔型樣
F(R)=R*mod(K)
F(R)：間隔型樣
R：第三私密質數
K：第二已知之加密鑰
404
剖析訊息內容且插入過多符號來
分散訊息內容於多個群組：
「123456」→「1002340056」

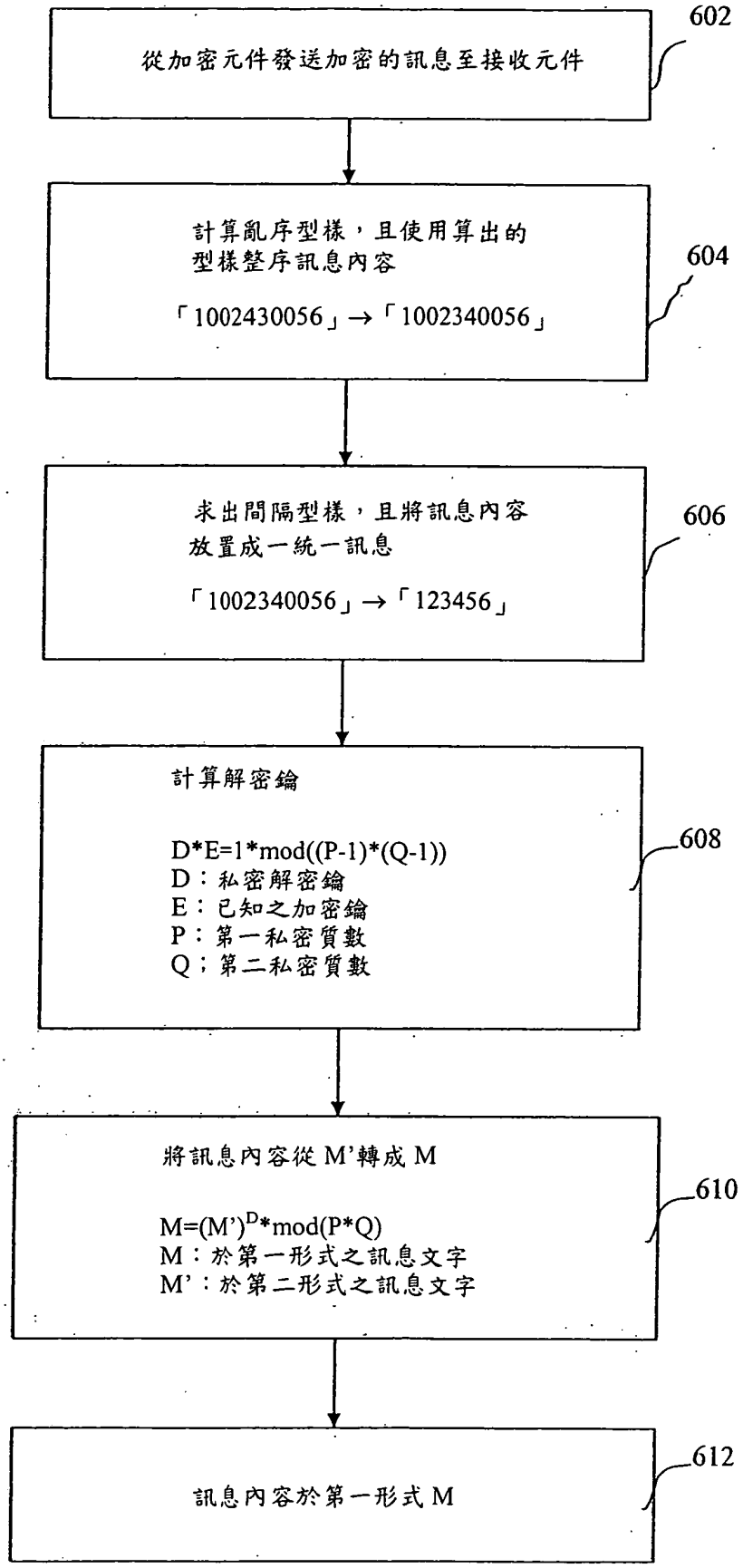
第 4a 圖


406
408
計算亂序型樣
G(S)=S*mod(J)
G(S)：亂序型樣
S：第黑私密質數
J：私密模數
410
剖析訊息內容且根據亂序型樣
亂序訊息內容：
「1002340056」→「1002430056」

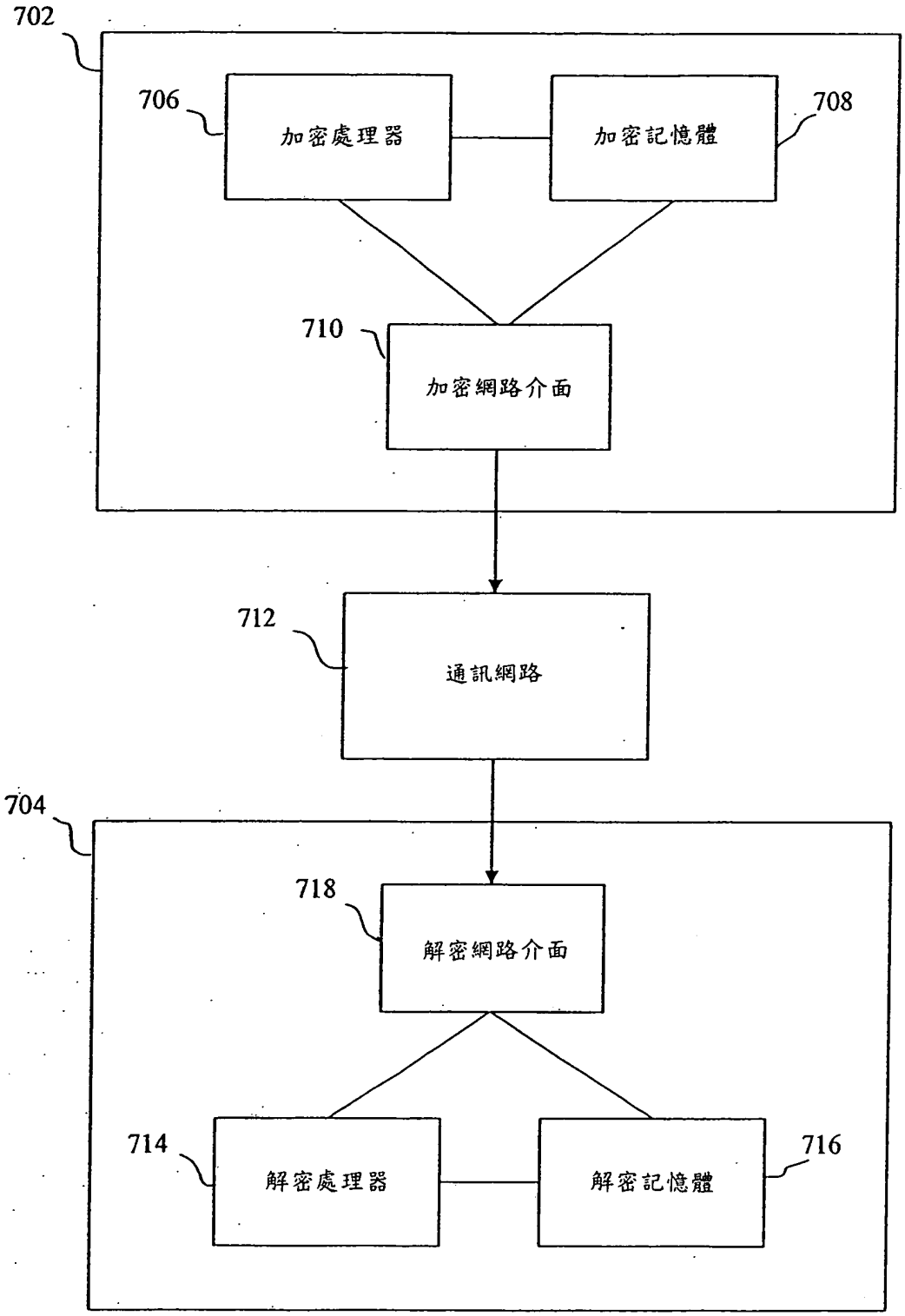
第 4b 圖


500
502
從加密元件發送加密的訊息至接收元件
504
計算亂序型樣，且使用算出的
型樣整序訊息內容
「1」__「243」__「56」→
「1」__「234」__「56」
506
求出間隔型樣，且將訊息內容
放置成一統一訊息
「1」__「234」__「56」→「123456」
508
計算解密鑰
D*E=1*mod((P-1)*(Q-1))
D：私密解密鑰
E：已知之加密鑰
P：第一私密質數
Q；第二私密質數
510
將訊息內容從 M'轉成 M'
M=(M')^D*mod(P*Q)
M：於第一形式之訊息文字
M'：於第二形式之訊息文字
512
訊息內容於第一形式 M

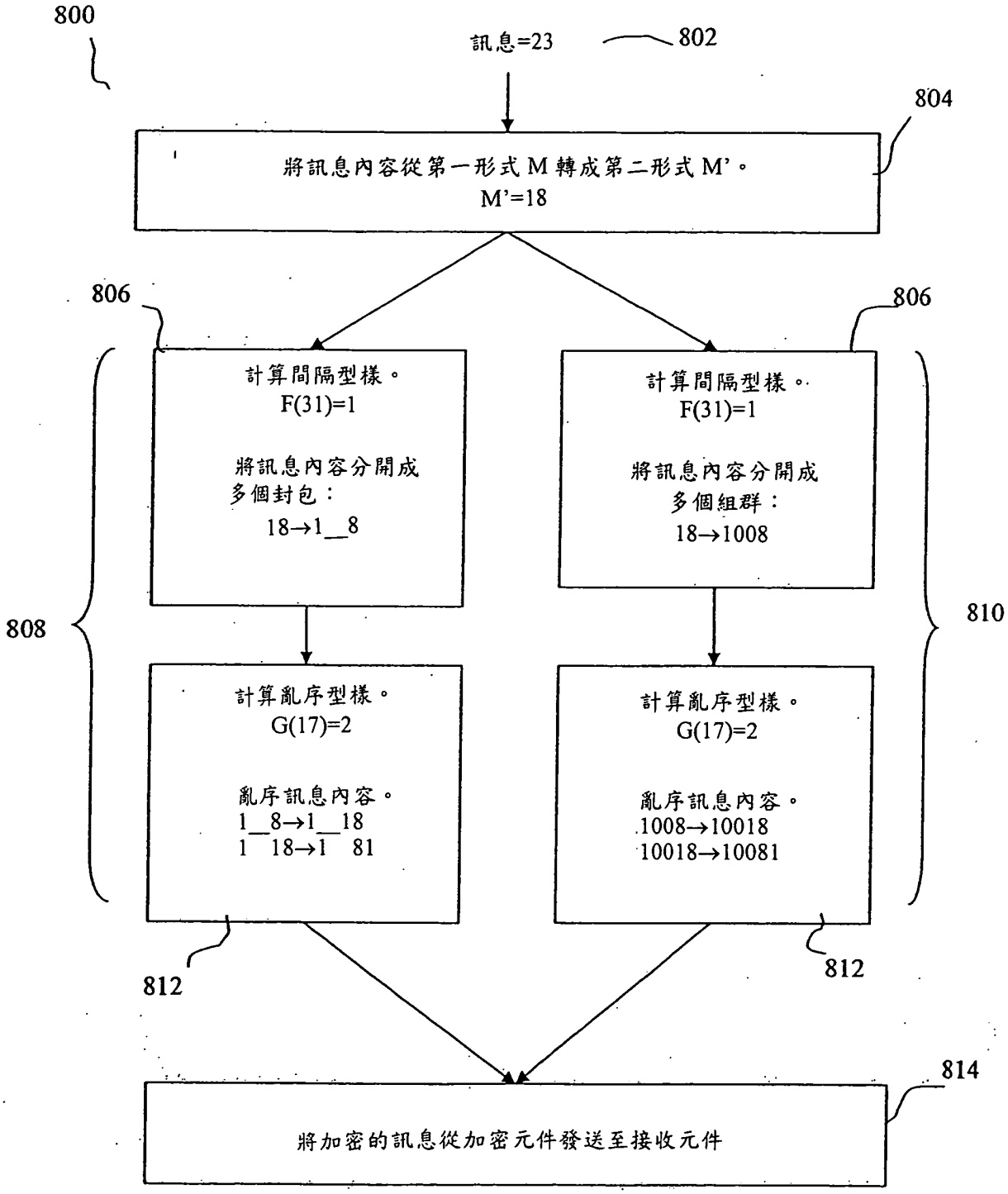
第 5 圖


600
602
從加密元件發送加密的訊息至接收元件
604
計算亂序型樣，且使用算出的
型樣整序訊息內容
「1002430056」→「1002340056」
606
求出間隔型樣，且將訊息內容
放置成一統一訊息
「1002340056」→「123456」
608
計算解密鑰
D*E=1*mod((P-1)*(Q-1))
D：私密解密鑰
E：已知之加密鑰
P：第一私密質數
Q；第二私密質數
610
將訊息內容從 M'轉成 M
M=(M')^D*mod(P*Q)
M：於第一形式之訊息文字
M'：於第二形式之訊息文字
612
訊息內容於第一形式 M

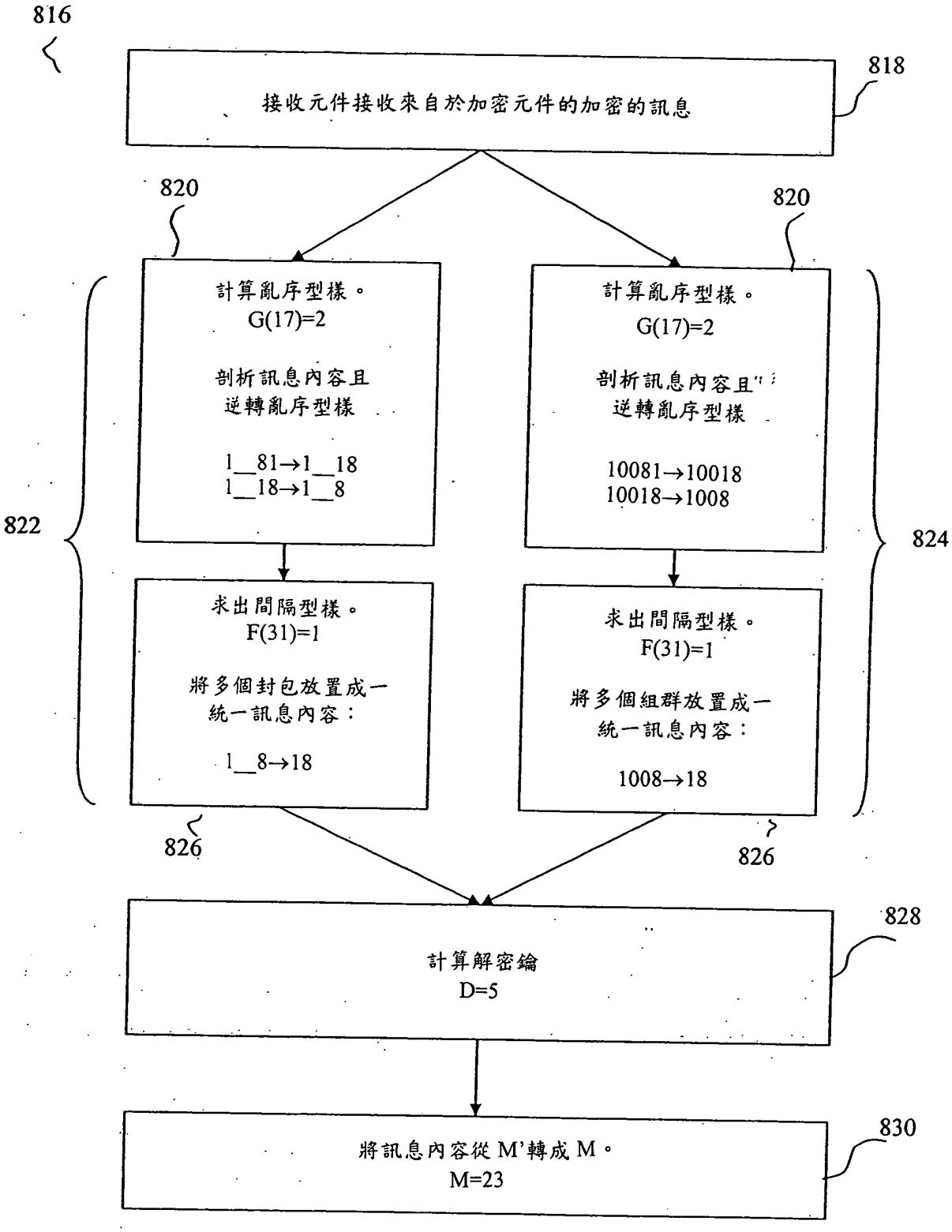
第 6 圖


702
706
加密處理器
加密記憶體
708
710
加密網路介面
712
通訊網路
704
718
解密網路介面
714
解密處理器
解密記憶體
716

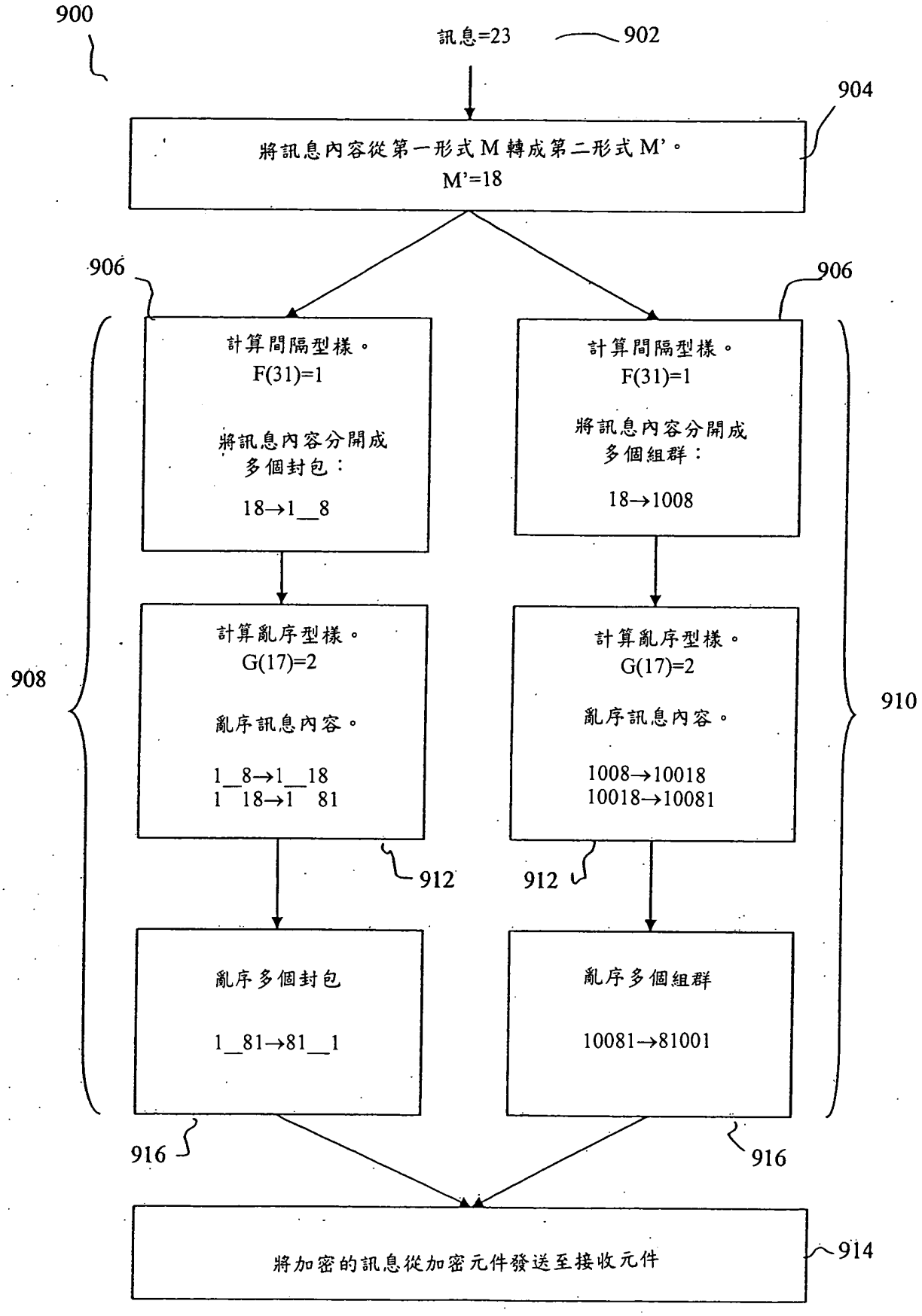
第 7 圖


800
訊息=23
802
804
將訊息內容從第一形式 M 轉成第二形式 M'。
M'=18
806
806
計算間隔型樣。
F(31)=1
將訊息內容分開成
多個封包：
18→1__8
計算間隔型樣。
F(31)=1
將訊息內容分開成
多個組群：
18→1008
808
810
計算亂序型樣。
G(17)=2
亂序訊息內容。
1__8→1__18
1 18→1 81
計算亂序型樣。
G(17)=2
亂序訊息內容。
1008→10018
10018→10081
812
812
814
將加密的訊息從加密元件發送至接收元件

第 8a 圖


816
接收元件接收來自於加密元件的加密的訊息
818
820
計算亂序型樣。
G(17)=2
剖析訊息內容且
逆轉亂序型樣
1__81→1__18
1__18→1__8
820
計算亂序型樣。
G(17)=2
剖析訊息內容且
逆轉亂序型樣
10081→10018
10018→1008
822
824
求出間隔型樣。
F(31)=1
將多個封包放置成一
統一訊息內容：
1__8→18
求出間隔型樣。
F(31)=1
將多個組群放置成一
統一訊息內容：
1008→18
826
826
計算解密鑰
D=5
828
將訊息內容從 M'轉成 M。
M=23
830

第 8b 圖


900
訊息=23
902
904
將訊息內容從第一形式 M 轉成第二形式 M'。
M'=18
906
906
計算間隔型樣。
F(31)=1
將訊息內容分開成
多個封包：
18→1__8
計算間隔型樣。
F(31)=1
將訊息內容分開成
多個組群：
18→1008
908
910
計算亂序型樣。
G(17)=2
亂序訊息內容。
1__8→1__18
1__18→1__81
計算亂序型樣。
G(17)=2
亂序訊息內容。
1008→10018
10018→10081
912
912
亂序多個封包
1__81→81__1
亂序多個組群
10081→81001
916
916
將加密的訊息從加密元件發送至接收元件
914

第 9 圖

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100...流程圖
102...三階段資料加密技術
104-111...動作方塊
112...三階段資料解密技術
114-118...動作方塊

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

十、申請專利範圍：

1. 一種用以加密訊息之方法，其包含下列步驟：

以一已知加密鑰E、一第一私密質數P、和一第二私密質數Q之函數，來將訊息的一內容從一第一形式M轉換成為一第二形式M'；

在轉換該訊息的該內容為該第二形式M'後，根據係至少一第三私密質數R之一函數的一間隔型樣，將該訊息的該經轉換內容分開以進一步加密該訊息的該內容；以及

在轉換該訊息的該內容為該第二形式M'後，根據係至少一第四私密質數S之一函數的一亂序型樣，將該訊息的該經轉換內容予以亂序以進一步加密該訊息之該內容。

2. 如申請專利範圍第1項之方法，進一步包含：

將該訊息之該內容從字母語法轉變成數值表示型態。

3. 如申請專利範圍第2項之方法，其中該訊息之該內容係使用一雜湊函數而從字母語法被轉換成為數值表示型態。

4. 如申請專利範圍第1項之方法，其中該已知加密鑰係與該第一私密質數和該第二私密質數互質。

5. 如申請專利範圍第4項之方法，其中該訊息之該內容係根據下式而從該第一形式M轉變成一第二形式M'：

$$M'=M^{E}\bmod(P^{*}Q)。$$

6. 如申請專利範圍第1項之方法，其中用以分開該訊息的該內容之該間隔型樣為根據下式之該第三私密質數R和模數K之函數：

$$F(R)=R^{*}\bmod(K)。$$

7. 如申請專利範圍第6項之方法，其中根據一間隔型樣分開該訊息的該內容之階段包含：

將該訊息的該內容脈衝化成為多個互異的封包。

8. 如申請專利範圍第6項之方法，其中根據一間隔型樣分開該訊息的該內容之階段包含：

將過量符號插入該訊息的該內容，來將該訊息的該內容分散至多群。

9. 如申請專利範圍第8項之方法，其中該等過量符號為空格。

10. 如申請專利範圍第1項之方法，其中該亂序型樣為根據下式的一私密模數J和該第四私密質數S之函數：

$$G(S)=S^{*}\bmod(J)。$$

11. 如申請專利範圍第1項之方法，進一步包含下列步驟：

於轉換該訊息的該內容、分開該訊息的該內容和亂序該訊息的該內容後，將一經加密訊息發送至一接收元件。

12. 一種加密與解密方法，其包含下列步驟：

以一已知加密鑰E、一第一私密質數P、和一第二私密質數Q之一函數，來將一訊息的一內容從一第一形式M轉換成為一第二形式M'；

在轉換該訊息的該內容為該第二形式M'後，根據一間隔型樣來分離該訊息的該經轉換內容以進一步加密該訊息之該內容，該間隔型樣為一第三私密質數R和一第二已知加密鑰K之函數；

在轉換該訊息的該內容為該第二形式M'後，根據一亂序型樣來亂序該訊息的該經轉換內容以進一步加密該訊息之該內容，該亂序型樣為一第四私密質數S和一私密模數J之函數；

從一加密元件發送一經加密的訊息至一接收元件；

計算該亂序型樣且剖析該經加密的訊息來逆轉該亂序型樣；

計算該間隔型樣且剖析該經加密的訊息來將該訊息的該內容置於一統一的訊息中；以及

以一解密鑰D、該第一私密質數P、及該第二私密質數Q之一函數來將該訊息的該內容由第二形式M'轉換成第一形式M。

13. 如申請專利範圍第12項之方法，其中該第一私密質數P與該第二私密質數Q之積係大於該訊息的該內容於第一形式M中之數值。

14. 如申請專利範圍第13項之方法，其中該已知加密鑰E係與該第一私密質數P與該第二私密質數Q互質。

15. 如申請專利範圍第14項之方法，其中該訊息的該內容係根據下式而從該第一形式M轉變成該第二形式M'：

$$M'=M^{E*} \bmod (P^*Q)。$$

16. 如申請專利範圍第12項之方法，其中該間隔型樣係根據下式計算：

$$F(R)=R^{*}\bmod(K)。$$

17. 如申請專利範圍第12項之方法，其中該亂序型樣係根據下式計算：

$$G(S)=S^{*}\bmod(J)。$$

18. 如申請專利範圍第12項之方法，其中該解密鑰係根據下式計算：

$$D^{*}E=1^{*}\bmod((P-1)^{*}(Q-1))。$$

19. 如申請專利範圍第18項之方法，其中該訊息的該內容係根據下式而從第二形式M'轉換成第一形式M：

$$M=(M')^{D*}\bmod(P^{*}Q)。$$

20. 一種用以加密訊息之系統，其包含下列步驟：

一加密模組，其包含一第一處理器、耦接該第一處理器之一第一記憶體、以及耦接一通訊網路、該第一處理器和該第一記憶體之一第一網路介面；

儲存於該第一記憶體且可藉第一處理器執行之轉換邏輯組件，來以一已知加密鑰E、一第一私密質數P及一私密質數Q之函數而將該訊息之一內容從一第一形式M轉換成一第二形式M'；

儲存於該第一記憶體且可由該第一處理器執行之分開邏輯組件，用來根據一間隔型樣而分開該訊息的該內容，以在該訊息的該內容被轉換為該第二形式M'後，進一步地加密該訊息的該內容；

儲存於該第一記憶體且可由該第一處理器執行之亂序邏輯組件，用來根據一亂序型樣而亂序該訊息之該內容，以在該訊息的該內容被轉換為該第二形式M'後，進一步地加密該訊息的該內容；以及

儲存於該第一記憶體且可由第一處理器執行之通訊邏輯組件，用來透過通訊網路發送一經加密的訊息。

21. 如申請專利範圍第20項之系統，其中該訊息之該內容係根據下式而從該第一形式M轉變成一第二形式M'：

$$M'=M^{E}\bmod(P^{*}Q)。$$

22. 如申請專利範圍第20項之系統，其中用以分開該訊息之該內容之間隔型樣為根據下式之一第三私密質數R和一模數K之一函數：

$$F(R)=R^{*}\bmod(K)。$$

23. 如申請專利範圍第22項之系統，其中根據一間隔型樣分開該訊息的該內容之階段包含：

將該訊息的該內容脈衝化成為多個分開的封包。

24. 如申請專利範圍第22項之系統，其中根據一間隔型樣分開該訊息的該內容之階段包含：

將過量符號插入該訊息之該內容，來將該訊息的該內容分散成多群。

25. 如申請專利範圍第20項之系統，其中該亂序型樣為根據下式的一私密模數J和一第四私密質數S之一函數：

$$G(S)=S^{*}\bmod(J)。$$

26. 一種用以加密與解密訊息之系統，包含：

轉換裝置，組配來以一已知加密鑰E、一第一私密質數P、和一第二私密質數Q之一函數，來將該訊息之一內容從一第一形式M轉換成為一第二形式M'；

分開裝置，組配來根據一間隔型樣來分開該訊息之該內容，以在該訊息的該內容被轉換為該第二形式M'後，進一步加密該訊息之該內容，該間隔型樣係一第三私密質數R和一第二已知加密鑰K之一函數；

亂序裝置，組配來根據一亂序型樣來亂序該訊息的該內容，以在該訊息的該內容被轉換為該第二形式M'後，進一步加密該訊息之該內容，該亂序型樣為一第四私密質數S和一私密模數J之一函數；

整序裝置，組配來計算該亂序型樣且剖析該經加密訊息來逆轉該亂序型樣；

統一裝置，組配來計算該間隔型樣以及剖析該經加密訊息，來將該訊息的該內容放置於一統一訊息內；以及

第二轉換裝置，組配來以一解密鑰D、該第一私密質數P及該第二私密質數Q之一函數，來將該訊息的該內容由該第二形式M'轉換成該第一形式M。

27. 如申請專利範圍第26項之系統，其中該第二轉換裝置係組配來根據下式，以該已知加密鑰E、第一私密質數P、及第二私密質數Q之一函數來計算該解密鑰D：

$$D^{*}E=1^{*}\mathrm{mod}((P-1)^{*}(Q-1))$$；以及

組配來使用該算出的解密鑰D並根據下式，將呈第

二形式M'的訊息內容轉回第一形式M：

$$M=(M')^{D}*\bmod(P*Q)。$$

28. 一種用以解密訊息之方法，其包含下列步驟：

接收一經加密訊息；

使用一亂序型樣，整序已基於該亂序型樣而被加密之該訊息的一內容；

使用一間隔型樣，將已基於一亂序型樣而被加密之該訊息的經分開內容放置成一統一訊息；以及

在整序該訊息之該內容以及放置該訊息之該內容為該統一訊息之後，基於一已知加密鑰E、一第一私密質數P、和一第二私密質數Q，將該訊息之該內容從一第二形式M'轉換回一第一形式M。

29. 如申請專利範圍之第28項之方法，其中整序該訊息的該內容之步驟包括下列步驟：

使用一第四私密質數S和一私密模數J，為該訊息的該內容計算該亂序型樣；

剖析該經加密的訊息以及反轉該亂序型樣；

其中該亂序型樣係根據下式來計算：

$$G(S)=S^{*}\bmod(J)。$$

30. 如申請專利範圍之第28項之方法，其中將該訊息的經分開內容放置成一統一訊息之步驟包含下列步驟：

使用一第三私密質數R和一第二已知加密鑰K，為該訊息的該內容計算該間隔型樣；以及

剖析該經分開訊息以反轉該間隔型樣；

其中該間隔型樣係根據下式來計算：

$$F(R)=R^{*}\bmod(K)。$$

31. 如申請專利範圍之第28項之方法，其中將該訊息之該內容從一第二形式M'轉換回一第一形式M之步驟包含下列步驟：

依該已知加密鑰E、第一私密質數P、和第二私密質數Q的一函數，計算一私密解密鑰D；以及

根據下式，使用該經計算私密解密鑰D來將該訊息的該內容從該第二形式M'轉換回該第一形式M：

$$M=(M')^{D*}\bmod(P^{*}Q)；$$

其中該私密解密鑰D係根據下式來計算：

$$D^{*}E=1^{*}\bmod((P-1)^{*}(Q-1))。$$

32. 一種用以解密訊息之系統，其包含：

一解密模組，其包含一處理器、與該處理器耦接之一記憶體、以及與一通訊網路、該處理器和該記憶體耦接之一網路介面；

儲存於該記憶體且可由該處理器執行之通訊邏輯組件，用來透過該通訊網路接收一經加密的訊息；

儲存於該記憶體且可由該處理器執行之整序邏輯組件，用以使用一亂序型樣，整序已基於該亂序型樣被加密之該訊息的一內容；

儲存於該記憶體且可由該處理器執行之統一邏輯組件，用以使用一間隔型樣，把已基於該間隔型樣被加

密之該訊息的分開內容放置於一統一訊息內；以及

儲存於該記憶體且可由該處理器執行之轉換邏輯組件，用以基於一已知加密鑰E、一第一私密質數P、和一第二私密質數Q，在該訊息的該內容被整序以及該訊息的該內容被放置於一統一訊息內之後，將該訊息的該內容從一第二形式M'轉換回為一第一形式M。

33. 如申請專利範圍之第32項之系統，其中該整序邏輯組件：

使用一第四私密質數S和一私密模數J，為該訊息的該內容計算該亂序型樣；以及

剖析該經加密的訊息以及反轉該亂序型樣；

其中該整序邏輯組件係根據下式來計算該亂序型樣：

$$G(S)=S^{*}\bmod(J)。$$

34. 如申請專利範圍之第32項之系統，其中該統一邏輯組件：

使用一第三私密質數R和一第二已知加密鑰K，為該訊息的該內容計算該間隔型樣；以及

剖析該經分開訊息以反轉該間隔型樣；

其中該統一邏輯組件根據下式來計算該間隔型樣：

$$F(R)=R^{*}\bmod(K)。$$

35. 如申請專利範圍之第32項之系統，其中該轉換邏輯組件：

依該已知加密鑰E、第一私密質數P、和第二私密質

數Q的一函數，來計算一私密解密鑰D；以及

根據下式，使用該經計算私密解密鑰D來將該訊息的該內容從該第二形式M'轉換回該第一形式M：

$$M=(M')^{D}*\mathrm{mod}(P*Q)；$$

其中該轉換邏輯組件根據下式來計算該私密解密鑰D：

$$D*E=1*\mathrm{mod}((P-1)*(Q-1))。$$