102年7月5日 修正補充

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：95107530

※ 申請日期：95.3.7　　※IPC 分類：G06F 21/60 (2013.01)
G06F 17/10 (2006.01)

一、發明名稱：（中文/英文）

資料處理裝置、資料處理系統、以及資料處理方法

二、申請人：（共１人）

姓名或名稱：（中文/英文）

NTI 股份有限公司

代表人：（中文/英文）中村貴利/NAKAMURA, TAKATOSHI

住居所或營業所地址：（中文/英文）

日本國三重縣四日市市松寺三丁目７番４號

國　籍：（中文/英文）日本/JAPAN

三、發明人：（共１人）

姓　名：（中文/英文）

中村貴利/TAKATOSHI NAKAMURA

國　籍：（中文/英文）

日本/JAPAN

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：　年　月　日。

☑ 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.日本、2005/03/08、2005-063271

☐ 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。

五、中文發明摘要：

本發明將資料處理裝置中的加密技術改良成使第三者解讀通訊的可能性進一步減少的裝置。

資料處理裝置加密處理目標資料以使之成為加密資料，將其記錄於既定的記錄媒體，並且，解密記錄於記錄媒體的該加密資料以復原成處理目標資料。進行加密時，將過去的解代入解產生用演算法，使用依次產生的解來產生用來加密的演算法和密鑰。解在之後不需要被代入解產生用演算法的階段被刪除。

六、英文發明摘要：

七、指定代表圖：

(一)本案指定代表圖為：第（9）圖。

(二)本代表圖之元件符號簡單說明：無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

九、發明說明：

【發明所屬之技術領域】

本發明是關於一種資料處理裝置及其應用，本發明可在加密純文字處理目標資料以使之成為加密資料之後，將其記錄於既定的記錄媒體，並解密從該記錄媒體讀取出來的加密資料。

【先前技術】

在資訊安全之重要性日益提高的今天，對於加密不宜讓第三者知道內容的資料(在本說明書中稱為「處理目標資料」)並將其記錄於記錄媒體中的上述資料處理裝置的需求變得非常大。為了得到處理目標資料的隱密性，有各式各樣的加密技術被提出並受到應用，不過，仍難以完全防止加密被解讀。

一般而言，處理目標資料的加密及在既定的記錄媒體上的記錄的進行方式為，每隔既定的位元數分割處理目標資料，各個被分割的資料被加密之後，合併成一個加密資料，再將其記錄於記錄媒體上。

當對每份分割處理目標資料之後的資料進行加密時，一般使用既定的演算法和密鑰。此演算法可防止加密被解讀，被設計得非常複雜，密鑰也受到嚴格的管理，以使外部無法知道。但是，無論將演算法設計得有多複雜或如何變更密鑰，一旦演算法和密鑰被人知道，解讀使用該演算法和密鑰來加密的資料將更容易。

另一方面，本發明之發明人不斷研究加密技術，率先研發出一種資料處理裝置，其包括一種可以連續產生用來加密和解密的演算法和密鑰中至少其中一者的裝置。

此技術可連續產生用來加密或解密的演算法和密鑰中至少其中一者，即使演算法和密鑰被知道了，之後也會變化演算法或密鑰或者變化兩者，所以，相較於過去的加密技術，其優點要好得多。

但是，在此技術中，當過去好幾個演算法或密鑰被知道時，有可能預測到該演算法或密鑰或兩者之後將如何變化，無法斷言被第三者解讀的可能性為零。

本發明以將一種資料處理裝置改良成通訊被第三者解讀的可能性減少的資料處理系統為課題，該資料處理系統加密純文字處理目標資料以使之成為加密資料，將其記錄於既定的紀錄媒體。

【發明內容】

有了解決有關的課題，本發明之發明人提出將在以下說明的第1發明、第2發明及第3發明。

本申請案之第1發明如下。

第1發明為一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其特徵

在於包括：解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，在既定的時序中依次產生新解；演算法產生裝置，使用所產生的解在既定的時序中依次產生新演算法；選定資訊記錄裝置，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

此資料處理裝置中的上述演算法產生裝置可在每次上述處理目標資料被加密或上述加密資料被解密時等既定時序，使上述演算法產生出來。另外，此資料處理裝置中的上述解產生裝置在使上述解產生出來的情況下，使用藉由將過去的解中的至少其中一個代入解產生用演算法而得到的既定的解，並且，在不需要重新代入的時點刪除過去的解。

換言之，在此資料處理裝置上，在加密和解密時所使用的演算法是在演算法產生裝置上連續產生的，不過，演算法產生裝置在產生演算法時用到了「解」。此解如上所述，使用過去的解所產生。並且，此解在不需要產生新解時被刪除。

於是，在此資料處理裝置上，過去的解一一被刪除，所以，即使得知目前這一刻的解，第三者也無法知道它是經由什麼樣的過程而產生的。

基於以上的理由，此資料處理裝置的加密通訊被第三者解讀的可能性很小。

上述的解最後亦可為虛擬亂數。

上述第 1 發明中的資料處理裝置使演算法產生變化，不過，亦可使密鑰產生變化。藉此，亦可得到和上述的情況相同的效果。

例如，一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其特徵在於包括：解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，在既定的時序中依次產生新解；密鑰產生裝置，使用所產生的解在既定的時序中依次產生新密鑰；選定資訊記錄裝置，將用來選定加密上述處理目標資料時所使用之上述密鑰的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

第 1 發明中的資料處理裝置亦可包括一分割裝置，其可每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，每隔和加密上述加密資料時所分割成之位元數相同的位元數分割該加密資料以使之成

為複數份加密分割資料，上述加密裝置在上述分割裝置上所分割的每個上述純文字分割資料上加密上述處理目標資料顛使之成為加密分割資料，並且，上述解密裝置在每個上述加密分割資料上解密上述加密資料以使之成為純文字分割資料，另外又包括一連接裝置，其連接在上述加密裝置所加密的複數份上述加密分割資料以使之成為連貫的加密資料，並且，連接上述解密裝置所解密的複數份上述純文字分割資料以使之成為連貫的處理目標資料。

包括演算法產生裝置的第 1 發明之資料處理裝置可以任何時序來產生演算法。

例如，上述演算法產生裝置可在每次進行上述處理目標資料的加密時產生演算法。若是如此，每當進行處理目標資料的加密時，產生了不同的演算法，於是，第三者難以類推出演算法。

上述演算法產生裝置可在每次上述純文字分割資料被加密時產生上述演算法。若是如此，演算法產生的頻率變大，於是，第三者更加難以類推出演算法。

包括密鑰產生裝置的第 1 發明之資料處理裝置可以任何時序來產生密鑰。

例如，上述密鑰產生裝置可在每次進行上述處理目標資料的加密時產生密鑰。若是如此，每當進行處理目標資料的加密時，產生了不同的密鑰，於是，第三者難以類推出密鑰。

上述密鑰產生裝置可在每次上述純文字分割資料被加

密時產生上述密鑰。若是如此，密鑰產生的頻率變大，於是，第三者更加難以類推出密鑰。

上述解產生裝置從過去的解產生新的解，不過，可將過去的複數個解代入上述解產生用演算法，以得到上述解。亦即，　可代入產生新解的解產生用演算法的過去的解可以是一個，也可以是複數個。

上述解產生裝置可保留一開始產生上述解時最先被代入上述解產生用演算法的初始解。

在包括演算法產生裝置之第 1 發明的資料處理裝置中所使用的選定資訊只要可以選定加密上述處理目標資料時所使用的上述演算法即可，可以是任何種類的資訊。

例如，上述選定資訊可為上述演算法本身，另外，也可為上述演算法產生裝置在產生上述演算法時所使用的上述解或者為顯示上述演算法產生裝置在產生上述演算法時所使用的上述解為第幾個產生的資訊。

在包括密鑰產生裝置之第 1 發明的資料處理裝置中所使用的選定資訊只要可以選定加密上述處理目標資料時所使用的上述密鑰即可，可以是任何種類的資訊。

例如，上述選定資訊可為上述密鑰本身，另外，也可為上述密鑰產生裝置在產生上述密鑰時所使用的上述解或者為顯示上述密鑰產生裝置在產生上述密鑰時所使用的上述解為第幾個產生的資訊。

和包括演算法產生裝置之第 1 發明的資料處理裝置相同的作用效果亦可以下面的方法得到。

此方法為一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄靦既定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟。

而且，上述資料處理裝置執行：步驟一，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，在既定的時序中依次產生新解；步驟二，使用所產生的解在既定的時序中依次產生新演算法；步驟三，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

和包括密鑰產生裝置之第 1 發明的資料處理裝置相同的作用效果亦可以下面的方法得到。

此方法為一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄靦既定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟。

而且，上述資料處理裝置執行：步驟一，將過去的解

代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，在既定的時序中依次產生新解；步驟二，使用所產生的解在既定的時序中依次產生密鑰；步驟三，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

本申請案之第 2 發明如下。

本申請案之第 2 發明為一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，其特徵在於包括：解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一演算法產生裝置，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；第二演算法產生裝置，產生與使用所產生的解在每次進行上述加密資料的解密時在上述第一演算法產生裝置上依次產生的演算法相同的新演算法；其中，上

述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

上述第 2 發明使演算法產生變化，不過，和第 1 發明的情況相同，也有使密鑰產生變化的情況。

在此情況下的第 2 發明為一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，其特徵在於包括：解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一密鑰產生裝置，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；第二密鑰產生裝置，產生與使用所產生的解在每次進行上述加密資料的解密時在上述第一密鑰產生裝置上依次產生的密鑰相同的新密鑰；其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

第 2 發明中的資料處理裝置和第 1 發明中的資料處理裝置類似，不過，使用了用來選定加密處理目標資料時所使用的演算法或密鑰的選定資訊。這和第 2 發明中的資料

處理裝置加密複數份處理目標資料以使之成為加密資料並且使用和加密複數份上述加密資料時相同的順序對其進行解密有關。

第 2 發明中的資料處理裝置的演算法產生裝置和密鑰產生裝置分別在每次處理目標資料被加密時，產生演算法或密鑰。另外，當第 2 發明中的資料處理裝置進行解密時，產生和加密時所使用的演算法及密鑰相同的演算法及密鑰。

於是，在第 2 發明中的資料處理裝置上，和過去所產生的演算法或密鑰相同的演算法或密鑰依序被產生，所以，若以和加密複數份上述加密資料時的相同順序解密該資料，不需要使用上述的選定資訊。

在以上的第 2 發明的兩個資料處理裝置上，設有第一演算法產生裝置及第二演算法產生裝置或第一密鑰產生裝置及第二密鑰產生裝置共用的一個解產生裝置，不過，亦可設置兩個分別與第一演算法產生裝置及第二演算法產生裝置或第一密鑰產生裝置及第二密鑰產生裝置對應的解產生裝置。

以前者為例，可以是一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其加密複數份處理目標資料以使之成為加密資料，並

且，使用和加密複數份上述加密資料時相同的順序對其進行解密，其特徵在於包括：第一解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一演算法產生裝置，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；第二解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；第二演算法產生裝置，產生與使用在上述第二解產生裝置上所產生的解在每次進行上述加密資料的解密時在上述第一演算法產生裝置上依次產生的演算法相同的新演算法；其中，上述第一解產生裝置及第二解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

以後者為例，可以是一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的解密裝置，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，其特徵在於包括：第一解產生裝置，將過去的解

代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一密鑰產生裝置，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；第二解產生裝置，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；第二密鑰產生裝置，產生與使用在上述第二解產生裝置上所產生的解在每次進行上述加密資料的解密時在上述第一密鑰產生裝置上依次產生的密鑰相同的新密鑰；其中，上述第一解產生裝置及第二解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

第 2 發明的資料處理裝置可包括一分割裝置，其可每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，每隔和加密上述加密資料時所分割成之位元數相同的位元數分割該加密資料以使之成為複數份加密分割資料，上述加密裝置在上述分割裝置上所分割的每個上述純文字分割資料上加密上述處理目標資料顯使之成為加密分割資料，並且，上述解密裝置在每個上述加密分割資料上解密上述加密資料以使之成為純文字分割資料，另外又包括一連接裝置，其連接在上述加密裝置所加密的複數份上述加密分割資料以使之成為連貫的加密資

料，並且，連接上述解密裝置所解密的複數份上述純文字分割資料以使之成為連貫的處理目標資料。

第 2 發明亦可以下面的方法來實現。

第 2 發明的第一個例子為一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄覦既定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟，其特徵在於：上述資料處理裝置執行：步驟一，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一演算法產生步驟，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；第二演算法產生步驟，產生與使用所產生的解在每次進行上述加密資料的解密時在上述第一演算法產生裝置上依次產生的演算法相同的新演算法；其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

第二個例子為一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄覦既

定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟，其特徵在於：上述資料處理裝置執行：步驟一，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一密鑰產生步驟，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；第二密鑰產生步驟，產生與使用所產生的解在每次進行上述加密資料的解密時在上述第一密鑰產生裝置上依次產生的密鑰相同的新密鑰；其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

第三個例子為.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄覦既定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟，其特徵在於：上述資料處理裝置執行：第一解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生

新解；第一演算法產生步驟，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；第二解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；第二演算法產生步驟，產生與使用在上述第二解產生裝置上所產生的解在每次進行上述加密資料的解密時在上述第一演算法產生裝置上依次產生的演算法相同的新演算法；其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

第四個例子為一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄覦既定的記錄裝置的步驟、使用加密從該記錄裝置讀取之加密資料時所使用的演算法及密鑰解密該加密資料以使之成為處理目標資料的步驟，其特徵在於：上述資料處理裝置執行：第一解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；第一密鑰產生步驟，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產

生新密鑰；第二解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；第二密鑰產生步驟，產生與使用在上述第二解產生裝置上所產生的解在每次進行上述加密資料的解密時在上述第一密鑰產生裝置上依次產生的密鑰相同的新密鑰；其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

本申請案的發明人亦提出以下的第 3 發明。

第 3 發明為一種資料處理系統，其結構包含複數個第一資料處理裝置、相同數目且與各個上述第一資料處理裝置對應的第二資料處理裝置及第三資料處理裝置，在上述第一資料處理裝置和上述第二資料處理裝置之間，進行純文字處理目標資料加密後的加密資料的通訊，並且，在上述第二資料處理裝置和上述第三資料處理裝置之間，進行處理目標資料上的通訊。

而且，上述第一資料處理裝置和上述第二資料處理裝置皆包括：分割裝置，每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，每隔和加密上述加密資料時所分割成之位元數相同的位元數分割該加密資料以使之成為複數份加密分割資料；　解產生裝

置，依次產生在對應之上述第一資料處理裝置和上述第二資料處理裝置上為共用且和其他上述第一資料處理裝置和上述第二資料處理裝置不同的解；加密解密裝置，藉由根據從上述解產生裝置接收之上述解所產生且在上述第一資料處理裝置和上述第二資料處理裝置上為共用的演算法加密上述純文字分割資料以使之成為加密分割資料，並且，藉由加密上述加密分割資料時所使用的演算法解密該加密資料以使之成為純文字分割資料；連接裝置，連接解密後的上述純文字分割資料以使之成為上述處理目標資料；收發裝置，收發上述加密資料；並且，上述第三資料處理裝置為申請專利範圍第 1 至 20 項中任一項之資料處理裝置，上述第二資料處理裝置加密解密在上述第一資料處理裝置上被加密的加密資料之後所產生的處理目標資料，將該加密資料記錄於上述記錄裝置，並且，解密從該記錄裝置讀取的加密資料，將之傳送至上述第二資料處理裝置。

【實施方式】

以下將一邊參照圖面，一邊詳細說明適用本發明的第1實施型態及第2實施型態。在第1實施型態及第2實施型態的說明中，在共通的部分使用共通的符號，省略了重複說明。

<第 1 實施型態>

此實施型態的資料處理系統大略具有如第 1 圖所示的結構。

資料處理系統包含透過網路 13 相互連接的複數個第

一資料處理裝置 11 及一個第二資料處理裝置 12。網路 13 在此實施型態中為 LAN（Local Area Network）。

複數個第一資料處理裝置 11 和第二資料處理裝置 12 相互進行加密通訊。

此外，網路 13 也可以為其他的結構，只要可以進行在第一資料處理裝置 11 和第二資料處理裝置 12 之間的資料交換即可。

在此說明第一資料處理裝置 11 和第二資料處理裝置 12 的結構。首先，說明第一資料處理裝置 11 的結構。

第一資料處理裝置 11 的硬體結構如第 2 圖所示。

第一資料處理裝置11在此實施型態中為包含CPU(central processing unit)21、ROM(read only memory)22、HDD(hard disk drive)23、RAM(random access memory)24、輸入裝置25、顯示裝置26、加密裝置27、通訊裝置28、匯流排29的結構。CPU21、ROM22、HDD23、RAM24、輸入裝置25、顯示裝置26、加密裝置27、通訊裝置28可透過匯流排29進行資料的交換。

在ROM22或HDD23中，記錄有既定的程式及既定的資料（其中，有時包含作為處理目標資料的內容，在本實施型態中為此種情況。另外，在既定的資料中，包含為了執行上述程式所需要的資料）。CPU21進行對整個第一資料處理裝置11的控制，根據儲存於ROM22或HDD23的程式、資料等，執行後述的處理。RAM24作為在CPU21進行處理時的作業用記憶區域來使用。

輸入裝置25由鍵盤、滑鼠等構成，用來輸入指令、資料等。顯示裝置26由LCD(liquid crystal display)、CRT(cathode ray tube)等構成，用來顯示指令、所輸入的資料、後述的處理狀況等。

加密裝置27進行後述的處理目標資料的加密及加密資料的解密。

通訊裝置28執行透過網路13且和第二資料處理裝置12之間的通訊。此外，第二資料處理裝置12的通訊裝置28執行透過網路13且和第一資料處理裝置11之間的通訊。

接著，說明通訊裝置28的結構。第3圖顯示通訊裝置28的方塊結構圖。

通訊裝置28由介面部281、認證資料產生部282及通訊部283構成。

介面部281進行匯流排29和通訊裝置28之間的資料交換。介面部281將從匯流排29接收的加密資料傳送至認證資料產生部282，將從通訊部283接收的加密資料傳送至匯流排29。

當認證資料產生部282將後述的加密資料傳送至第二資料處理裝置12時，在欲傳送的加密資料的標頭中，附加認證資料。認證資料選定傳送加密資料的第一資料處理裝置11。認證資料經由第二資料處理裝置12的管理者等在每個第一資料處理裝置11受到分割，例如，記錄於ROM22或HDD23中。認證資料產生部282在加密資料上附加從ROM22或HDD23讀取的認證資料。第二資料處理裝置12如後所述，

藉由在所接收的加密資料上所附加的認證資料，可確認該加密資料從哪一個第一資料處理裝置11被傳送。認證資料產生部282將附加認證資料的加密資料傳送至通訊部283。通訊部283將所接收的加密資料傳送至第二資料處理裝置12。

接著，說明加密裝置27的結構。第4圖顯示加密裝置27的方塊結構圖。

加密裝置27由介面部271、前處理部272、加密解密部273、解產生部274、演算法產生部275、密鑰產生部276及連接部277構成。

介面部271進行匯流排29和通訊裝置28之間的資料交換。

介面部271透過匯流排29，從HDD23接收處理目標資料，另外，透過匯流排29，從通訊部28接收加密資料，將所接收的處理目標資料或加密資料傳送至前處理部272。另外，當介面部271接收處理目標資料或加密資料時，將顯示其內容的資料傳送至解產生部274。

另一方面，介面部271如後所述，從連接部277接收處理目標資料或加密資料，將所接收的處理目標資料或加密資料傳送至匯流排29。

前處理部272具有一功能，其將透過介面部271從匯流排29所接收的處理目標資料或加密資料分割成既定的位元數，產生純文字分割資料或加密分割資料，再將其傳送至加密解密部273。處理目標資料或加密資料的分割方式將會

在後面敘述。此外，前處理部272在此實施型態中具有一功能，其在處理目標資料中以後述的方法包含與處理目標資料無關的資料亦即虛擬資料。

加密解密部273具有一功能，其從前處理部272接收純文字分割資料或加密分割資料，當接收純文字分割資料時，對其加密，當接收加密分割資料時，對其解密。此外，此實施型態中的加密解密部273固定加密解密時的處理單位亦即基準位元數。此實施型態中的基準位元數基本上不受限制，在此的範例為8位元。加密及解密的處理細節將會在後面敘述。

解產生部274依序產生解。第一資料處理裝置11的解產生部274所產生的解同於後述的第二資料處理裝置12的解產生部274A所產生的解和以相同順序所產生的解。此實施型態中的解為虛擬亂數。所產生的解被傳送至前處理部272、演算法產生部275和密鑰產生部276。

演算法產生部275根據從解產生部274所接收的解產生演算法。此演算法在加密解密部273進行加密處理及解密處理時被使用。

密鑰產生部276根據從解產生部274所接收的解產生密鑰。此密鑰在加密解密部273進行加密處理及解密處理時被使用。

連接部277具有一功能，其將在加密解密部273解密加密分割資料所產生的純文字分割資料以原來的順序連接成一份處理目標資料。此處理目標資料被傳送至介面部271，

透過匯流排29，根據需要，被傳送至HDD23或CPU21等。連接部277另外具有一功能，其將在加密解密部273加密純文字分割資料所產生的加密分割資料連接成一份加密資料。此加密資料被傳送至介面部271，之後，透過匯流排29被傳送至通訊裝置28的通訊部283，然後進一步從通訊部283被傳送至第二資料處理裝置12。此外，連接部277亦可不具有連接在加密解密部273加密純文字分割資料而產生的加密分割資料的功能。在此情況下，加密分割資料依照被加密的順序依次被傳送至對方的通訊裝置中。在連接部277為此種裝置的情況下，加密分割資料可不通過連接部277，直接被傳送至通訊部283。

接著，說明第二資料處理裝置12的結構。

第二資料處理裝置12的硬體結構如第5圖所示。

第二資料處理裝置12的硬體結構基本上和第一資料處理裝置11相同，不過，在第一資料處理裝置11上為一個的加密裝置27有兩種，設置了加密裝置27A加密裝置27B來取代加密裝置27，此點和第一資料處理裝置11不同。

第二資料處理裝置12中的CPU21、ROM22、HDD23、RAM24、輸入裝置25、顯示裝置26、匯流排29和第一資料處理裝置11中的相同。

加密裝置27A、加密裝置27B和第一資料處理裝置11中的加密裝置27相同，具有對處理目標資料加密和對加密資料解密的功能。以下將依序說明兩邊的結構。

加密裝置27A為複數個，和第一資料處理裝置11具有相

同的數目，每一個裝置對應設置在每一個第一資料處理裝置11上。亦即，互相對應設置的加密裝置27A和第一資料處理裝置11可解密對方加密處理目標資料所產生的加密資料。反之，不互相對應設置的加密裝置27A和第一資料處理裝置11無法解密對方加密處理目標資料所產生的加密資料。

加密裝置27A具有如第6圖所示的結構。

加密裝置27A由介面部271A、前處理部272A、加密解密部273A、解產生部274A、演算法產生部275A、密鑰產生部276A及連接部277所構成。

介面部271A透過匯流排29，從加密裝置27B接收處理目標資料，另外，透過匯流排29，從通訊部28接收加密資料，將所接收的處理目標資料或加密資料傳送至前處理部272A。另外，當介面部271A接收處理目標資料或加密資料時，將顯示其內容的資料傳送至解產生部274A。

另一方面，介面部271A如後所述，從連接部277A接收處理目標資料或加密資料，將所接收的處理目標資料或加密資料傳送至匯流排29。

前處理部272A具有一功能，其將透過介面部271A從匯流排29所接收的處理目標資料或加密資料分割成既定的位元數，產生純文字分割資料或加密分割資料，再將其傳送至加密解密部273A。前處理部272A在此實施型態中具有一功能，其在處理目標資料中以後述的方法包含與處理目標資料無關的資料亦即虛擬資料。

加密解密部273A具有一功能，其從前處理部272A接收純文字分割資料或加密分割資料，當接收純文字分割資料時，對其加密，當接收加密分割資料時，對其解密。此外，此實施型態中的加密解密部273A固定加密解密時的處理單位亦即基準位元數。此實施型態中的基準位元數基本上不受限制，在此的範例為8位元。加密及解密的處理細節將會在後面敘述。

解產生部274A依序產生解。此解產生部274A所產生的解同於第一資料處理裝置11的解產生部274所產生的解和以相同順序所產生的解。所產生的解被傳送至前處理部272A、演算法產生部275A和密鑰產生部276A。

演算法產生部275A根據從解產生部274A所接收的解產生演算法。此演算法在加密解密部273A進行加密處理及解密處理時被使用。第二資料處理裝置12中的演算法產生部275A所產生的演算法和在第一資料處理裝置11中的演算法產生部275以相同順序產生的演算法相同。

密鑰產生部276A根據從解產生部274A所接收的解產生密鑰。此密鑰在加密解密部273A進行加密處理及解密處理時被使用。第二資料處理裝置12中的密鑰產生部276A所產生的密鑰和在第一資料處理裝置11中的密鑰產生部276上以相同順序產生的密鑰相同。

第二資料處理裝置12中的連接部277A的功能和第一資料處理裝置11相同。連接部277A將在加密解密部273A解密加密分割資料所產生的純文字分割資料以原來的順序連接

成一份，產生處理目標資料。此處理目標資料透過匯流排29被傳送加密裝置27B。連接部277A又將加密解密部273A加密純文字分割資料所產生的加密分割資料連接成一份，產生加密資料。此加密資料透過通訊裝置28，被傳送至第一資料處理裝置11。

加密裝置27B只有一個。

加密裝置27B具有一功能，其可再度加密第一資料處理裝置11加密處理目標資料所產生的加密資料又受到加密裝置27A解密而產生的處理目標資料。加密裝置27B將所產生的加密資料記錄於第二資料處理裝置12內的HDD23內。另外，加密裝置27B具有一功能，其解密從該HDD23讀取的加密資料。

加密裝置27B具有如第7圖所示的結構。

加密裝置27B由介面部271B、前處理部272B、加密解密部273B、解產生部274B、演算法產生部275B、密鑰產生部276B、連接部277B及選定資訊產生部278B所構成。

加密裝置27B的介面部271B透過匯流排29，從加密裝置27A接收處理目標資料，另外，透過匯流排29，從第二資料處理裝置12內的HDD23接收加密資料，將所接收的處理目標資料或加密資料傳送至前處理部272B。另外，當介面部271B接收處理目標資料或加密資料時，將顯示其內容的資料傳送至解產生部274B。

另一方面，介面部271B如後所述，從加密裝置27B的連接部277B接收處理目標資料，從選定資訊產生部278B接收

加密資料，將所接收的處理目標資料或加密資料傳送至匯流排29。

前處理部272B具有一功能，其將透過介面部271B從匯流排29所接收的處理目標資料或加密資料分割成既定的位元數，產生純文字分割資料或加密分割資料，再將其傳送至加密解密部273B。前處理部272B在此實施型態中具有一功能，其在處理目標資料中以後述的方法包含與處理目標資料無關的資料亦即虛擬資料。

加密解密部273B具有一功能，其從前處理部272B接收純文字分割資料或加密分割資料，當接收純文字分割資料時，對其加密，當接收加密分割資料時，對其解密。此外，此實施型態中的加密解密部273B固定加密解密時的處理單位亦即基準位元數。此實施型態中的基準位元數基本上不受限制，在此的範例為8位元。加密及解密的處理細節將會在後面敘述。此外，當此加密解密部273B進行解密時，使用根據後述的選定資訊所選定的演算法及密鑰來進行解密。

解產生部274B依序產生解。此解產生部274B所產生的解為虛擬亂數。所產生的解被傳送至演算法產生部275B、密鑰產生部276B。在此實施型態中，被傳送至前處理部272B。

演算法產生部275B根據從解產生部274B所接收的解產生演算法。此演算法在加密解密部273B進行加密處理及解密處理時被使用。

密鑰產生部276B根據從解產生部274B所接收的解產生密鑰。此密鑰在加密解密部273B進行加密處理及解密處理時被使用。第二資料處理裝置12中的密鑰產生部276B所產生的密鑰和在第一資料處理裝置11中的密鑰產生部276上以相同順序產生的密鑰相同。

第二資料處理裝置12中的連接部277B具有一功能，其連接加密解密部273B解密加密分割資料所產生的純文字分割資料以產生處理目標資料。此處理目標資料被傳送加密裝置27A。連接部277B又將加密解密部273B加密純文字分割資料所產生的加密分割資料連接成一份，產生加密資料。此加密資料被記錄於第二資料處理裝置12內的HDD23內。

在加密裝置 27B 中，包含選定資訊產生部 278B。

選定資訊產生部 278B 在連接部 277B 所產生的加密資料中附加選定資訊。此選定資訊為用來選定加密附加有該選定資料之加密資料時所使用之演算法和密鑰的資訊。具體來說，其為顯示加密該加密資料時所使用的演算法本身、加密該加密資料時所使用的密鑰本身、加密該加密資料時所使用之演算法或密鑰被產生出時所使用的解本身或該解為第幾個產生的解的資訊。此外，在此實施型態中，演算法和密鑰兩者一起變化，所以，選定資訊必須選定演算法和密鑰兩者或者選定為了產生演算法和密鑰而使用的解或該解被產生的順序，不過，當只有演算法和解的其中一者不產生變化時，選定資訊可僅選定演算法或解的變化。

此外，在此實施型態中，選定資訊產生部 278B 在加密

資料中附加選定資訊，不過，亦可另外在與加密資料不同的地方進行和加密資料對應的設置來儲存選定資訊。

第二資料處理裝置 12 中的通訊裝置 28 的結構和第一資料處理裝置 11 中的通訊裝置 28 的結構約略相同。介面部 281、通訊部 283 的功能和第一資料處理裝置 11 的通訊裝置 28 中的一樣。第二資料處理裝置 12 的通訊裝置 28 包括認證部 284，取代第一資料處理裝置 11 中的認證資料產生部 282，這點和第一資料處理裝置 11 的通訊裝置 28 不同。

認證部 284 在從第一資料處理裝置 11 接收加密資料的此實施型態中，讀取標頭中所包含的認證資料，判斷該加密資料是哪一個第一資料處理裝置 11 傳來。加密資料透過介面部 281，被傳送至與該傳送來源亦即第一資料處理裝置 11 對應設置的加密裝置 27A。

接著，說明在此資料處理系統上進行的處理流程。

若使用第 9 圖作概略說明，在此資料處理系統上進行的處理流程如下。

首先，複數個第一資料處理裝置 11 中的一個第一資料處理裝置 11 的加密裝置 27 加密處理目標資料，產生加密資料(S110)。

其次，該第一資料處理裝置 11 將該加密資料送至該第二資料處理裝置 12(S120)。

接著，在接收加密資料的第二資料處理裝置 12 內的複數個加密裝置 27A 中與送來該加密資料的第一資料處理裝置 11 對應設置者解密該加密資料，使之復原成處理目標資

料(S130)。

接著，解密之後的該處理目標資料由加密裝置 27B 加密，記錄於第二資料處理裝置 12 內的 HDD23 內(S140)。

接著，根據來自第一資料處理裝置 11 的請求，HDD23 內的加密資料被加密裝置 27B 解密，復原成處理目標資料(S150)。

接著，該處理目標資料被加密裝置 27A 加密，成為加密資料(S160)。

接著，該加密資料被第二資料處理裝置 12 傳送至第一資料處理裝置(S170)。

接著，該加密資料被第一資料處理裝置 11 內的加密裝置 27 解密，復原成原來的處理目標資料(S180)。

上述 S110 的步驟為，複數個第一資料處理裝置 11 中的一個第一資料處理裝置 11 的加密裝置 27 加密處理目標資料，產生加密資料，首先，一邊參照第 10 圖，一邊詳細說明上述 S110 的步驟。

首先，進行處理目標資料的讀取(S1101)。處理目標資料可為從從第一資料處理裝置 11 傳送至第二資料處理裝置 12 所需要的資料。在此實施型態中，處理目標資料被記錄於 HDD23。從外部記錄媒體等其他記錄媒體讀取至第一資料處理裝置 11 的資料可作為處理目標資料。

例如，當輸入從輸入裝置 25 將處理目標資料傳送至第二資料處理裝置 12 這種內容的指令時，CPU21 從 HDD23 讀取處理目標資料，將其暫時記錄於 RAM24。此處理目標資

料從 HDD23 經由匯流排 29，被傳送至介面部 271。更進一步詳細地說，此處理目標資料透過介面部 271，被傳送至前處理部 272。

在前處理部 272，處理目標資料被分割成既定的位元數，變成純文字分割資料(S1102)。前處理部 272 根據需要，在純文字分割資料中包含虛擬資料。

從處理目標資料產生純文字分割資料的方法可為一種，不過，在此實施型態中，可藉由以下三種方法中的任何一種從處理目標資料產生純文字分割資料。

A) 將處理目標資料分割成比基準位元數少的既定位元數，以使之成為純文字分割資料，並且，在每個在位元數少於基準位元數的純文字分割資料中的既定位置包含虛擬資料

B) 將處理目標資料分割成比基準位元數少的既定位元數，以使之成為純文字分割資料，並且，在每個在位元數少於基準位元數的純文字分割資料中的不同位置包含虛擬資料

C) 將處理目標資料分割成等於或少於基準位元數的既定位元數，以使之成為純文字分割資料，並且，在每個在位元數少於基準位元數的純文字分割資料中包含虛擬資料

藉由使用上述三種方法中的任何一個，是否從處理目標資料產生純文字分割資料，可藉由解產生部 274 所產生的解來決定。

因此，在此先說明解產生部 274 如何產生解。

解產生部 274 當介面部 271 從匯流排 29 接收處理目標資料時，從介面部 271 接收該資訊。

解產生部 274 趁此機會開始產生解。在此實施型態中，解產生部 274 每當處理目標資料在介面部 271 被接收時，產生解。此外，在本發明中解不受此限制，但作為此實施型態的範例，解為 8 行 8 列陣列(X)。

解產生部 274 不一定要是這樣，在此實施型態中，解以非線性遷移的方式連續產生。此解最後為虛擬亂數。

若要以非線性遷移的方式連續產生解，可考慮(1)在解的產生步驟中包含過去的解的乘冪運算、(2)在解的產生步驟中，包含過去的兩個以上的解的相乘或組合(1)和(2)等的手法。

在此實施型態中，解產生部 274 在初始陣列方面，預先設定並儲存為第０１解（X_{01}）和第０２解（X_{02}）(例如，第０１解（X_{01}）和第０２解（X_{02}）被記錄於 HDD23、ROM22 等既定的記憶體中)。各個第一資料處理裝置 11 所具有的初始陣列互異，所以，在各個第一資料處理裝置 11 上所產生的解也互異。

此外，第二資料處理裝置 12 中的複數個加密裝置 27A 的每一個都具有和與各個加密裝置 27A 對應設置之第一資料處理裝置 11 所具有的加密裝置相同的初始陣列。

解產生部 274 將此初始陣列代入解產生用演算法，以下面的方式產生第１解（X_1）。

第１解（X_1）＝$X_{02}X_{01}+\alpha$（α＝８行８列的陣

列）

此為最初產生的解。

接著，當介面部 271 從匯流排 29 接收處理目標資料時，解產生部 274 以下面的方式產生第 2 解（X_2）。

第 2 解（X_2）＝$X_1X_{02}+\alpha$

同樣地，每當介面部 271 從匯流排 29 接收處理目標資料時，解產生部 274 以下面的方式產生第 3 解、第 4 解、…第 N 解。

第 3 解（X_3）＝$X_2X_1+\alpha$

第 4 解（X_4）＝$X_3X_2+\alpha$

：

第 N 解（X_N）＝$X_{N-1}X_{N-2}+\alpha$

以此方式產生的解被傳送至前處理部 272、演算法產生部 275 及密鑰產生部 276，並且，被儲存於解生部 274。在此實施型態中，為了產生第 N 解（X_N），需要第 N－1 解（X_{N-1}）と第 N－2 解（X_{N-2}），使用離目前最近的在其之前所產生的兩個解。於是，當解產生部 274 使生新的解時，必須儲存離目前最近的過去所產生的兩個解（或者，非解產生部 274 的其他裝置必須儲存這兩個解）。反之，比離目前最近的過去所產生的兩個解還早產生的解為產生新的解時使用不到的東西。因此，在此實施型態中，常常將最近的過去兩個解儲存於解產生部 274，當產生新的解時，將已經曾為第 2 個解而目前變成第 3 個解的解從記錄該解的既定記憶體等中刪除。

此外，以此種方式產生的解為非線性遷移的高斯解，為虛擬亂數。

若要產生非線性遷移，當求第 N 解時，除了使用上述第 N 解（X_N）＝$X_{N-1}X_{N-2}+\alpha$ 這個數學式以外，還可使用下面的數學式。

例如，

（a）第 N 解（X_N）＝（X_{N-1}）^{P}

（b）第 N 解（X_N）＝（X_{N-1}）^{P}（X_{N-2}）^{Q}（X_{N-3}）^{R}（X_{N-4}）^{S}

（c）第 N 解（X_N）＝（X_{N-1}）^{P}＋（X_{N-2}）^{Q}

此外，P、Q、R、S 分別為既定的常數。另外，當使用數學式(a)或(c)時，解產生部 274 具有 2 個初始陣列，當使用數學式(b)時，解產生部 274 具有 4 個初始陣列。

另外，上述 α 為常數，不過，亦可作為對其作選定變化的環境資訊。此環境資訊為經過一段時間會依序自然產生的資訊，亦為可使相隔兩地的地點共用並取得的資訊，例如，根據選定地區的天氣來決定的資訊、根據在選定的時間播放的電視台的電視播放內容來決定的資訊、根據選定的體育運動的比賽結果來決定的資訊等。

若從此種環境資訊依序製作上述 α 來產生共用資訊，可進一步提高通訊的隱密性。

在上述數學式(a)~(c)的右邊，當然也可以加上 α（此可從環境資訊產生）。

如上所述，接收解(亦即上述的解)的前處理部 272 據

此決定要以上述的 A)、B)、C)中哪一個方法來產生純文字分割資料。在此實施型態中，不限制此點，不過作為範例，加上解構成 8 行 8 列陣列的數字之後的和再除以 3，當得到的餘數為 0 時，使用 A)方法，當餘數為 1 時，使用 B)方法，當餘數為 2 時，使用 C)方法，分別產生純文字分割資料。

當使用 A)方法產生純文字分割資料時，前處理部 272 將從介面部 271 接收的處理目標資料依序從前端分割成比基準位元數少的既定位元數(在此實施型態中為 7 位元)，藉此，產生出純文字分割資料。另外，前處理部 272 在純文字分割資料的既定位置埋入虛擬資料。此外，埋入虛擬資料的純文字分割資料的位置可變化，亦可固定。在後者的情況下，埋入虛擬資料的位置可為純文字分割資料的前端、末端或第 2 位元、第 3 位元等的既定的中間位置。此虛擬資料可為任何一種和處理目標資料無關的資料。例如，常會考慮埋入 0 資料或 1 資料或交替埋入 0 和 1 資料的處理。甚至有其他的例子可根據上述的解來決定埋入哪一種虛擬資料。例如，將加上解亦即構成 8 行 8 列陣列的數字之後的和除以 9，當得到的餘數為 0 時，埋入 0, 0, 0, 0…這樣連續為 0 的資料，當餘數為 1 時，埋入 0, 1, 0, 1…這樣每隔 1 位數就插入 1 的資料，當餘數為 2 時，埋入 0, 0, 1, 0, 0, 1…這樣每隔 2 位數就插入 1 的資料，同樣，當餘數為 3 時，埋入每隔 3 位數就插入 1 的資料，當餘數為 4 時，埋入每隔 4 位數就插入 1 的資料，…當餘數為 9

時，埋入每隔 9 位數就插入 1 的資料。

當使用 B)方法產生純文字分割資料時，前處理部 272 將處理目標資料分割成比基準位元數少的既定位元數(例如 7 位元)，以使之成為純文字分割資料，並且，在每個在位元數少於基準位元數的純文字分割資料中的不同位置包含虛擬資料。在此情況下，埋入虛擬資料的位置可為固定，在各個純文字分割資料上，可以第 1 位元、第 2 位元、第 3 位元…第 8 位元、第 1 位元、第 2 位元、第 3 位元…第 8 位元這樣的順序移動，作有規則的變化，或者，作隨意的變化。在埋入虛擬資料的位置為隨意變化的情況下，埋入虛擬資料的位置可根據解來決定。

根據解來決定埋入虛擬資料的位置的方法可為，將加上解亦即構成 8 行 8 列陣列的數字之後的和除以 8，當所得到的餘數為 0 時，每隔一份純文字分割資料，在前端和末端交替埋入虛擬資料，當餘數為 1 時，在前端埋入虛擬資料的純文字分割資料和在末端埋入虛擬資料的純文字分割資料相隔 2 份資料，當餘數為 2 時，在前端埋入虛擬資料的純文字分割資料和在末端埋入虛擬資料的純文字分割資料相隔 3 份資料，…當餘數為 7 時，在前端埋入虛擬資料的純文字分割資料和在末端埋入虛擬資料的純文字分割資料相隔 8 份資料，以此方式進行處理。如同前端和末端，亦可不固定埋入虛擬資料的位置，進一步移動該位置。

當使用 C)方法產生純文字分割資料時，將處理目標資料分割成少於或等於基準位元數的位元數。此分割可將處

理目標資料分割成比 8 位元少的任意長度，例如，將加上解亦即構成 8 行 8 列陣列的數字之後的和除以 8，當所得到的餘數為 0 時，將處理目標資料的該時點的前端部分分割成 8 位元，當餘數為 1 時，將處理目標資料的該時點的前端部分分割成 1 位元，當餘數為 2 時，將處理目標資料的該時點的前端部分分割成 2 位元，…當餘數為 7 時，將處理目標資料的該時點的前端部分分割成 7 位元。另外，前處理部 272 在藉此產生的純文字分割資料中的位元數比基準位元數少的較短純文字分割資料中，埋入虛擬資料。在此情況下的虛擬資料的埋入位置可為前端、末斷等選定位置，例如，可為根據解來選定而會變化的既定位置。

無論如何，以此種方式產生的純文字分割資料依照產生的順序以串流的方式傳送至加密解密部 273。

和純文字分割資料的產生同時，演算法產生部 275 產生加密純文字分割資料時所使用的演算法。

此實施型態中的演算法產生部 275 根據解產生演算法。

在此實施型態中，演算法產生部 275 以下面的方式產生演算法。

此實施型態中的演算法被定義為『將 8 位元的純文字分割資料當作 1 行 8 列的陣列 Y 之後，對解亦即 8 行 8 列陣列 X 乘以 a 之後，僅依順時針方向旋轉 n×90°，再乘以 Y』。

在此，a 有時被設定為既定的常數，不過，在此實施

型態中，為根據解來變化的數字。亦即，此實施型態中的演算法根據解來變化。例如，a 的決定方式可根據將加上 8 行 8 列陣列的解中所包含的所有陣列元素之後所得到的數除以 5 之後的餘數(不過，當餘數為 0 時，a=1)。

另外，上述 n 為根據密鑰來決定的既定的數。若密鑰為既定的數，n 則固定，不過，如以下所說明的，密鑰會根據解來變化。亦即，在此實施型態中，此 n 亦根據解來變化。

不過，亦可將演算法決定成其他的形式。

在此實施型態中，演算法產生部 275 每當從解產生部 274 接收解時，便產生演算法，然後將其傳送至加密解密部 273。

和純文字分割資料的產生同時，密鑰產生部 276 產生加密純文字分割資料時所使用的密鑰。

密鑰產生部 276 根據密鑰來產生解。

在此實施型態中，密鑰產生部 276 可以下面的方式產生密鑰。

此實施型態中的密鑰加上 8 行 8 列陣列的解所包含的所有陣列元素所得到的數。於是，密鑰在此實施型態中根據解來變化。

此外，密鑰亦可決定為其他形式。

在此實施型態中，密鑰產生部 276 每當從解產生部 274 接收解時，便產生密鑰，然後將其傳送至加密解密部 273。

加密解密部 273 根據從演算法產生部 275 接收的驗算

法和從密鑰產生部 276 接收的密鑰來加密從前處理部 272 接收的純文字分割資料(S1103)。

演算法如上所述，決定的方式為『將 8 位元的純文字分割資料當作 1 行 8 列的陣列 Y 之後，對解亦即 8 行 8 列陣列 X 乘以 a 之後，僅依順時針方向旋轉 n×90°，再乘以 Y』，密鑰 n 則為上述的數。

例如，當 a 為 3 且 n 為 6 時，將 X 乘以 3 所得到的 8 行 8 列陣列僅依照順時針方向旋轉 6×90°=540°，再對如此得到的 8 行 8 列陣列，乘以純文字分割資料，以進行加密。

藉此所產生的資料為加密分割資料。

加密分割資料被傳送至連接部 277。連接部 277 將加密分割資料連接成一份資料，產生加密資料(S1104)。此時的加密分割資料的排列順序和原來的純文字分割資料的排列順序對應。

如上所述，首先，第一資料處理裝置 11 加密處理目標資料以產生加密資料的 S110 的步驟結束。

以此方式所產生的加密資料透過匯流排 29 被傳送至第一資料處理裝置 11 內的通訊裝置 28。加密資料被通訊裝置內的介面部 281 接收，被傳送至認證資料產生部 282。認證資料產生部 282 將認證資料附加在加密資料的標頭上，然後將加密資料傳送至通訊部 283。

通訊部 283 透過網路 13 將該加密資料傳送至第二資料處理裝置 12。藉此，上述 S120 的步驟被執行。

在接收此加密資料的第二資料處理裝置 12 中，解密加

密資料以使之復原成處理目標資料的 S130 的步驟被執行。

以下一邊參照第 11 圖，一邊詳述此解密的步驟。

傳送至第二資料處理裝置 12 的加密資料由第二資料處理裝置 12 的通訊裝置 28 中的通訊部 283 接收(S1201)。

通訊部 283 將此加密資料傳送至認證部 284。認證部 284 根據附加於該加密資料的認證資料來判斷該加密資料使從哪一個第一資料處理裝置 11 傳送過來(S1202)。

由認證部 284 進行相關的判斷後，該加密資料被傳送至介面部 281。介面部 281 將該加密資料傳送至在認證部 284 被判斷為該加密資料的傳送來源的第一資料處理裝置 11 所對應的加密裝置 27A。

加密裝置 27A 內的前處理部 272A 透過介面部 271A 接收此加密資料。

前處理部 272A 將所接收的加密資料分割成既定的位元數，產生加密分割資料(S1203)。

當分割加密資料以產生加密分割資料時，前處理部 272A 進行和在第一資料處理裝置 11 的連接部 277 上所進行的處理相反的處理。亦即，加密資料從前端被分割成以 8 位元為單位，被分為複數份加密分割資料。

接著，加密分割資料被傳送至加密解密部 273A，在此解密，變成純文字分割資料(S1204)。

解密以第一資料處理裝置 11 中的加密解密部 273 上所進行的處理相反的處理來執行。為此，在第二資料處理裝置 12 上需要在第一資料處理裝置 11 上進行加密時所需要

的演算法和密鑰。

解密時所使用的演算法和密鑰在加密裝置 27A 內產生。在此說明其結構。

加密裝置 27A 的介面部 271A 接收加密資料這個訊息的資訊被傳送至解產生部 274A。解產生部 274A 以接收此資訊為運作時機，每接收此資訊，便產生解。

在第二資料處理裝置 12 的加密裝置 27A 內的解產生部 274A 上所進行的解的產生是以和在第一資料處理裝置 11 的解產生部 274 上所進行的相同步驟來進行。此外，此解產生部 274A 如上所述，具有和包含該產生部 274A 的加密裝置 27A 所對應的第一資料處理裝置 11 的解產生部 274 所具有的初始陣列相同的初始陣列和解產生用演算法。於是，若比較在第二資料處理裝置 12 的加密裝置 27A 內所產生的解和以相同順序產生者，在對應的第一資料處理裝置 11 的加密裝置 27 內所產生的解相同。

所產生的解從解產生部 274A 被傳送至前處理部 272A、演算法產生部 275A 和密鑰產生部 276A。

演算法產生部 275A 根據所接收的解，在每次接收解時產生演算法。第二資料處理裝置 12 的演算法產生部 275A 產生演算法的步驟和第一資料處理裝置 11 的演算法產生部 275 產生演算法的步驟相同。所產生的演算法從演算法產生部 275A 被傳送至加密解密部 273A。

另一方面，密鑰產生部 276A 根據所接收的解，在每次接收解時產生密鑰。第二資料處理裝置 12 的密鑰產生部

276A 產生密鑰的步驟和第一資料處理裝置 11 的密鑰產生部 276 產生密鑰的步驟相同。所產生的密鑰從密鑰產生部 276A 被傳送至加密解密部 273A。

不過，在此資料處理系統中，每當在第一資料處理裝置 11 上進行加密，在第一資料處理裝置 11 上便產生新的解，而且，每當在第一資料處理裝置 11 上所產生的加密資料在第二資料處理裝置 12 上被解密，在第二資料處理裝置 12 上被產生新的解。另外，如上所述，若比較在第二資料處理裝置 12 的加密裝置 27A 上所產生的解和以相同順序產生者，和在對應的第一資料處理裝置 11 內的加密裝置 27 上所產生解相同。於是，在第一資料處理裝置 11 上加密某份處理目標資料時所產生的解和根據該解所產生的演算法及密鑰全都常常和使用該解所產生的演算法及密鑰被使用在第一資料處理裝置 11 上所產生的加密資料要被解密時在第二資料處理裝置 12 的加密裝置 27A 上所產生的解和根據該解所產生的演算法及密鑰一致。此外，此情況在第二資料處理裝置 12 上進行加密且在第一資料處理裝置 11 上進行解密的情況相同。

在加密解密部 273A 上，如上所述，使用從演算法產生部 275A 接收的演算法來進行解密的處理。更詳細地說，加密解密部 273A 根據從演算法產生部 275A 所接收的演算法(被定義為『將 8 位元的純文字分割資料當作 1 行 8 列的陣列 Y 之後，對解亦即 8 行 8 列陣列 X 乘以 a 之後，僅依順時針方向旋轉 n×90°，再乘以 Y，如此所求得的即為加密

分割資料』），產生用來進行解密處理的演算法（被定義為『將8位元的純文字分割資料當作1行8列的陣列Z之後，對解亦即8行8列陣列X乘以a之後，僅依順時針方向旋轉n×90°，得到反陣列，對其乘以Y，所求得的即為純文字分割資料』），使用密鑰進行根據上述定義的運算，藉此，進行解密的處理。如此，在加密解密部273A上，依次解密從前處理部272A以串流方式供給的加密分割資料，產生純文字分割資料。

接著，加密解密部273A根據需要，從純文字分割資料除去虛擬資料（S1205）。如上所述，在解產生部274A所產生的解被傳送至前處理部272A。此解是在第一資料處理裝置11的前處理部272決定如何將虛擬資料埋入純文字分割資料中時被使用的。亦即，加密裝置27A的前處理部272A在該時點所擁有的解顯示第二資料處理裝置12的加密解密部273A如何將虛擬資料埋入完成解密（或者進行解密或將要解密）的加密分割資料中（更正確地說，該加密分割資料被加密前的純文字分割資料）。

前處理部272A將在加密解密部273解密後的純文字分割資料的何處埋入虛擬資料的資訊傳送至加密解密部273A。

加密解密部273A使用此資訊，從純文字分割資料之中除去虛擬資料。

以此種方式所產生的純文字分割資料被傳送至連接部277A。連接部277A將所接收的純文字分割資料連接成一份

資料，將其復原成在第一資料處理裝置 11 上加密之前的原來狀態的處理目標資料(S1206)。

如此，第二資料處理裝置 12 解密加密資料以使之復原成處理目標資料的步驟 S130 結束。

所產生的處理目標資料從連接部 277A 被傳送至介面部 271A，透過匯流排 29 傳送至加密裝置 27B。

在此，加密裝置 27B 進行再度加密解密後的該處理目標資料以使之成為加密資料的上述 S140 的處理。

加密裝置 27B 中的加密處理以和第一資料處理裝置 11 中的流程約略相同的流程來進行(第 12 圖)。

傳送至加密裝置 27B 的處理目標資料由介面部 271B 接收(S1301)。

介面部 271B 將其傳送至前處理部 272B。

前處理部 272B 將所接收的處理目標資料分割成既定的位元數，產生純文字分割資料(S1302)。在此情況下的處理目標資料的分割方式不需要和加密裝置 27 及加密裝置 27A 相同，不過，在此實施型態中，進行和在加密裝置 27 及加密裝置 27 中所說明的處理相同的處理，藉此，分割處理目標資料。另外，前處理部 272B 進行和在加密裝置 27 中所說明過的處理相同的處理，根據需要在純文字分割資料中包含虛擬資料。

接著，純文字分割資料被傳送至加密解密部 273B，在此加密，變成加密分割資料(S1303)。

在此，和加密裝置 27 的情況相同，產生用來加密的演

算法及密鑰。在此之前，和產生解的加密裝置 27 的情況相同。以下說明從產生解到產生演算法及密鑰的流程。

當解產生部 274B 從匯流排 29 接收處理目標資料時，從介面部 271B 接收該資訊。解產生部 274B 可在適當的時序產生解，不過，此實施型態中的解產生部 274B 將從介面部 271B 接收已接收處理目標資料這個訊息的資訊作為產生解的時機來產生解。解的產生細節和在加密裝置 27 中所說明過的相同。

所產生的解被傳送至演算法產生部 275B 和密鑰產生部 276B。

演算法產生部 275B 和密鑰產生部 276B 進行和加密裝置 27 中的演算法產生部 275 和密鑰產生部 276 所執行的處理相同的處理，來產生演算法和密鑰。所產生的演算法和密鑰從演算法產生部 275B 或密鑰產生部 276B 傳送至加密解密部 273B。

加密解密部 273B 從演算法產生部 275B 接收演算法，從密鑰產生部 276B 接收密鑰，根據它們，依序加密從前處理部 272B 所接收的純文字分割資料(S1303)。

加密的細節和在加密裝置 27 中所說明的相同。

所產生的加密分割資料依序被傳送至連接部 277B。

連接部 277B 將加密分割資料變成一份，使之成為加密資料(S1304)。此加密資料被傳送至選定資訊產生部 278B。

選定資訊產生部 278B 在所接收的加密資料的標頭之類的地方附加上述的選定資訊(S1305)。

附加選定資訊的加密資料透過介面部 271B 被傳送至匯流排 29，記錄於第二資料處理裝置 12 內的 HDD23。

接著，在從第一資料處理裝置 11 回應記錄於第二資料處理裝置 12 內的 HDD23 的加密資料的指示到來的情況下，第二資料處理裝置 12 執行以下的處理。

首先，加密裝置 27B 執行上述 S150 的處理，亦即，從 HDD23 讀取加密資料，解密該加密資料以使之復原成處理目標資料。此處理的細節將一邊參照第 13 圖來說明。

具體來說，第二資料處理裝置 12 的加密裝置 27B 中的介面部 271B 從 HDD23 透過匯流排 29 讀取加密資料(S1401)。

介面部 271B 將此加密資料傳送至前處理部 272B。前處理部 272B 將所接收的加密資料分割成既定的位元數，產生加密分割資料(S1402)。

當分割加密資料以產生加密分割資料時，前處理部 272B 進行和在進行解密時加密裝置 27A 的前處理部 272A 所進行的上述處理相同的處理。亦即，加密資料從前端被分割成每 8 位元為一單位，分成複數份加密分割資料。

接著，加密分割資料依序被傳送至加密解密部 273B，在那裡解密，變成純文字分割資料(S1403)。

解密是執行和進行解密時加密裝置 27A 的加密解密部 273A 所進行的上述處理相同的處理。為了進行相關的解密，在第二資料處理裝置 12 上，需要演算法和密鑰。

演算法和密鑰以下面的方式來產生。

此實施型態中的介面部 271B 加密資料上所附加的選定資訊。此選定資訊是用來選定加密附加該選定資訊之加密資料時所使用的演算法和密鑰的。

例如，在選定資訊為加密該加密資料時所使用的演算法和密鑰本身的情況下，介面部 271B 從加密資料讀取此演算法和密鑰，透過前處理部 272B 將其傳送至加密解密部 273B。加密解密部 273B 根據此演算法和密鑰，進行加密分割資料的解密。

另外，當選定資訊為產生加密該加密資料時所使用之演算法和密鑰時所使用的解時，介面部 271B 從加密資料讀取此解，將其傳送至演算法產生部 275B 和密鑰產生部 276B。在此情況下，演算法產生部 275B 和密鑰產生部 276B 根據所接收的解，分別產生演算法和密鑰，不過，此演算法和密鑰分別和加密附加該解之加密資料時所使用的演算法及密鑰一致。演算法產生部 275B 和密鑰產生部 276B 將所產生的演算法和密鑰傳送至加密解密部 273B。加密解密部 273B 根據此演算法和密鑰，進行加密資料的解密。

另外，當選定資訊為顯示產生加密該加密資料時所使用之演算法和密鑰時所使用的解圍第一個產生的解的資訊時，介面部 271B 從加密資料讀取此資訊，將其傳送至解產生部 274B。接收此資訊的解產生部 274B 依照其所示的順序產生解。此解和加密附加上述資訊之加密資料時所使用的解一致。此外，在此情況下，為了使以相同順序產生的解常常相同，不刪除初始陣列而將之保留下來。解產生部

274B 將所產生的解傳送至演算法產生部 275B 和密鑰產生部 276B。演算法產生部 275B 和密鑰產生部 276B 根據所接收的解，分別產生演算法和密鑰，不過，此演算法和密鑰分別和加密附加該解之加密資料時所使用的演算法及密鑰一致。演算法產生部 275B 和密鑰產生部 276B 將所產生的演算法和密鑰傳送至加密解密部 273B。加密解密部 273B 根據此演算法和密鑰，進行加密分割資料的解密。

如上所述，加密分割資料復原成純文字分割資料。

接著，加密解密部 273B 根據需要，從純文字分割資料除去虛擬資料(S1404)。

在此，若純文字分割資料中所包含的虛擬資料根據解被包含在適當的位置，當加密解密部 273B 除去虛擬資料時，需要上次加密該純文字分割資料時所使用的解。當選定資訊為上次加密該純文字分割資料時所使用的解時，介面部 271B 將此解傳送至加密解密部 273B。另外，當選定資訊為顯示上次加密該純文字分割資料時所使用的解為第一個產生的解的資訊時，解產生部 274B 將所產生的解傳送至加密解密部 273B。使用此解，加密解密部 273B 根據解除去被包含在適當位置的虛擬資料。

此外，當純文字分割資料中所包含的虛擬資料根據解被包含在適當位置時，不宜將選定資訊設定為加密該加密資料時所使用的演算法和密鑰本身。如此，加密解密部 273B 無法得到解，所以，無法去除虛擬資料。

去除了虛擬資料的純文字分割資料被傳送至連接部

277B。此純文字分割資料在連接部 277B 被變成一份，復原成連續的處理目標資料(S1405)。

此純文字分割資料透過介面部 271B 被傳送至匯流排 29，又被傳送至要求傳送此純文字分割資料原來的加密資料的第一資料處理裝置 11 對的加密裝置 27A。

接收資料的加密裝置 27A 執行上述 S160 的處理，亦即，加密該處理目標資料以使之成為加密資料。

加密裝置 27A 當加密處理目標資料時，將此處理作為和第一資料處理裝置 11 的加密裝置 27 所進行的且在 S110 中所說明過的處理相同的處理來執行。

在加密裝置 27A 上所產生的加密資料透過匯流排 29 被傳送至第二資料處理裝置 12 中的通訊裝置 28，然後，透過網路 13，被傳送至委託傳送加密資料的第一資料處理裝置 11 的通訊部 28。此對應於上述 S170 的處理。

此加密資料在第一資料處理裝置 11 內的加密裝置 27 上被解密。此為上述 S180 的處理。此外，加密裝置 27 當將此加密資料解密為處理目標資料時，將此處理作為第二資料處理裝置 12 的加密裝置 27A 所進行的且在 S130 中所說明過的處理相同的處理來執行。

總之，此實施型態中的每一個第一資料處理裝置 11 上所內建的加密裝置 27 和內建該加密裝置 27 的第一資料處理裝置 11 對應的第二資料處理裝置 12 內的加密裝置 27A 可相互解密對方所加密的加密資料。

在第一資料處理裝置 11 內的加密裝置 27 上所解密而

產生的處理目標資料和進行 S110 的處理之前的第一資料處理裝置 11 內的 HDD23 的相同。此處理目標資料被記錄於第一資料處理裝置 11 內的 HDD23 內。第一資料處理裝置 11 可適當使用該資料。

<第 2 實施型態>

在第 2 實施型態中，資料處理裝置只有一個。

第 2 實施型態中的資料處理裝置的硬體結構和第 1 實施型態中的第一資料處理裝置 11 相同。不過，第 2 實施型態中的資料處理裝置不需要通訊，所以，不具有第一資料處理裝置 11 所包括的通訊裝置 28。

亦即，第 2 實施型態中的資料處理裝置包括 CPU21、ROM22、HDD23、RAM24、輸入裝置 25、顯示裝置 26、加密裝置 27、匯流排 29。這些構造的各個功能基本上和第一資料處理裝置 11 中的 CPU21、ROM22、HDD23、RAM24、輸入裝置 25、顯示裝置 26、加密裝置 27、匯流排 29 的功能相同。

不過，第 2 實施型態中的資料處理裝置的加密裝置 27 的結構和第 1 實施型態的第一資料處理裝置中所內建的加密裝置 27 的結構(第 4 圖所示的構造)幾乎相同，其中，演算法產生部 75 換成第一演算法產生部 275X 及第二演算法產生部 275Y，密鑰產生部 276 換成第一密鑰產生部 276X 及第二密鑰產生部 276Y，只有這一點和第 1 實施型態的加密裝置 27 不同(第 14 圖)。

在第 2 實施型態的資料處理裝置中，如後所述，進行

加密裝置27加密記錄於HDD23的處理目標資料、將該加密所產生的加密資料記錄於HDD23、加密裝置27解密記錄於HDD23的加密資料、將該解密所產生的處理目標資料記錄於HDD23的各種處理，不過，在第2實施型態中，被解密的加密資料為複數份，而且，加密資料被解密的順序和加密資料從處理目標資料被加密的順序一致。

第2實施型態中的資料處理裝置的加密裝置27和第1實施型態的第一資料處理裝置11中所內建的加密裝置27的不同點與這一點有關。

第2實施型態中的資料處理裝置的加密裝置27如上所述，具有如第14圖所示的結構。

第2實施型態中的資料處理裝置內的加密裝置27所具有的介面部271、前處理部272、加密解密部273、解產生部274及連接部277基本上和第1實施型態的第一資料處理裝置11的加密裝置27內的那些構造具有相同的功能。介面部271進行匯流排29和通訊裝置28之間的資料交換。

前處理部272透過介面部271將從匯流排29接收的處理目標資料或加密資料分割成既定的位元數，產生純文字分割資料或加密分割資料，再將其傳送至加密解密部283。前處理部272有時會在純文字分割資料中包含虛擬資料。

加密解密部273從前處理部272接收純文字分割資料或加密分割資料，當接收純文字分割資料時，將其加密，當接收加密分割資料時，將其解密。加密解密部273在此實施型態中，將加密及解密時的處理單位亦即基準位元數

固定為 8 位元。

解產生部 274 依序產生解。在此實施型態中，解在每一前處理部 272 接收處理目標資料時被產生。解為虛擬亂數。

連接部 277 具有一功能，其可將在加密解密部 273 解密加密分割資料而產生的純文字分割資料依照原來的順序連接成一份處理目標資料。連接部 277 又具有一功能，其可將在加密解密部 273 加密純文字分割資料而產生的加密分割資料依照原來的順序連接成一份加密資料。

第一演算法產生部 275X 根據從解產生部 274 所接收的解產生演算法。此演算法在進行加密時被使用。第二演算法產生部 275Y 根據從解產生部 274 所接收的解產生演算法。此演算法在進行解密時被使用。此外，當第一演算法產生部 275X 和第二演算法產生部 275Y 使用相同的解產生演算法時，會產生相同的演算法。

第一密鑰產生部 276X 根據從解產生部 274 所接收的解產生密鑰。此密鑰在進行加密時被使用。第二密鑰產生部 276Y 根據從解產生部 274 所接收的解產生密鑰。此密鑰在進行解密時被使用。此外，當第一密鑰產生部 276X 和第二密鑰產生部 276Y 使用相同的解產生密鑰時，會產生相同的密鑰。

在此實施型態中，第一演算法產生部 275X 及第一密鑰產生部 276X 在每一次前處理部 272 接收處理目標資料時產生演算法和密鑰。另外，第二演算法產生部 275Y 及第二密

鑰產生部276Y在每一次前處理部272接收加密資料時產生演算法和密鑰。

第2實施型態中的資料處理裝置的運作在這裡使用第5圖來說明。

首先，進行處理目標資料的讀取(S1501)。處理目標資料在此實施型態中從HDD23被讀取出來。處理目標資料從HDD23經過匯流排29，被傳送至加密裝置27。更詳細地說，此處理目標資料透過介面部271，被傳送至前處理部272。

在前處理部272，處理目標資料被分割成既定的位元數，變成純文字分割資料(S1502)。前處理部272根據需要在純文字分割資料中包含虛擬資料。

從處理目標資料產生純文字分割資料的方法和第1實施型態的S1102中所說明過的相同。

另一方面，解產生部274從介面部271以接收介面部271接收了處理目標資料這個資訊為運作時機來產生解。此外，解可在每當處理目標資料在前處理部272被分割時被產生。在此情況下，前處理部272的處理目標資料的產生和解產生部274的解的產生為同步。

此實施型態中的解的產生的方法和第1實施型態中的第一資料處理裝置11進行加密時的解產生部274所進行的相同。

所產生的解被傳送至第一演算法產生部275X、第二演算法產生部275Y、第一密鑰產生部276X及第二密鑰產生部276Y。

接收該解的第一演算法產生部 275X 及第一密鑰產生部 276X 分別產生演算法和密鑰。此實施型態中的演算法及密鑰的產生方法和第 1 實施型態的第一資料處理裝置 11 產生演算法和密鑰時的演算法產生部 275X 及第一密鑰產生部 276X 所進行的相同。

第一演算法產生部 275X 及第一密鑰產生部 276X 將所產生的演算法和密鑰傳送至加密解密部 273。

另外，加密解密部 273 根據從第一演算法產生部 275X 所接收的演算法和從第一密鑰產生部 276X 所接收的密鑰，加密從前處理部 272 所接收的純文字分割資料(S1503)。此處理作為和在第 1 實施型態中所說明過的 S1103 的處理相同的處理來進行。

藉此所產生的加密分割資料被傳送至連接部 277，在那裡被連接成一份，成為加密資料(S1504)。

如上所述，所產生的加密資料透過匯流排 29 被記錄於資料處理裝置內的 HDD23。

此種加密處理在此實施型態中進行複數次。

在此資料處理裝置中，進行記錄於 HDD23 中的加密資料的解密。

以下參照第 16 圖詳述解密的步驟。

解密從加密裝置 27 讀取記錄於 HDD23 中的加密資料開始(S1601)。

當加密裝置 27 內的前處理部 272 透過介面部 271 從 HDD23 接收加密資料時，前處理部 272 將所接收的加密資

料分割成既定的位元數，產生加密分割資料(S1602)。

當分割加密資料以產生加密分割資料時，前處理部 272 進行和在上述的加密處理中所進行的處理相反的處理。亦即，加密資料從前端被分割成以 8 位元為一單位，分成複數份加密分割資料。此處理和第 1 實施型態中的 S1203 的處理相同。

接著，加密分割資料被傳送至加密解密部 273，在那裡被解密，變成純文字分割資料(S1603)。

解密作為和在加密解密部 273 所進行的上述加密處理相反的處理來執行。為此，加密解密部 273 需要加密時所使用的演算法和密鑰。在此，使用先前產生的解，分別使第二演算法產生部 275Y 產生演算法，第二密鑰產生部 276Y 產生密鑰。加密資料被解密的順序和加密資料從處理目標資料被加密的順序一致，所以，第二演算法產生部 275Y 和第二密鑰產生部 276Y 所產生的演算法和密鑰根據欲解密的加密資料被加密時所使用的解來產生。此意味著，第二演算法產生部 275Y 所產生的演算法和第二密鑰產生部 276Y 所產生的密鑰與之後欲解密的加密資料被加密時所使用的演算法和密鑰一致。

此外，第二演算法產生部 275Y 和第二密鑰產生部 276Y 亦可在解產生部 274 產生解之後，為了解密，以加密解密部 273 需要演算法和密鑰的時序來產生演算法和密鑰。

第二演算法產生部 275Y 所產生的演算法和第二密鑰產生部 276Y 所產生的密鑰被傳送至加密解密部 273。加密

解密部 273 使用該演算法和密鑰依次解密加密分割資料以使之成為純文字分割資料。此處理作為和在第 1 實施型態的 S1204 中所說明過的處理相同的處理來執行。

接著，加密解密部 273 根據需要，從純文字分割資料除去虛擬資料(S1604)。此處理作為和在第 1 實施型態的 S1205 的處理相同的處理來執行。

以此方式所產生的純文字分割資料被傳送至連接部 277。連接部 277 將所接收的純文字分割資料連接成一份資料，產生處理目標資料(S1605)。

所產生的處理目標資料從連接部 277 被傳送至介面部 271，透過匯流排 29 被記錄於 HDD23。

<變形例>

第 2 實施型態中的資料處理裝置可有如下的變形。

此變形例中的資料處理裝置和第 2 實施型態中的資料處理裝置及加密裝置的結構有些不同。至於其他部分，則與上述第 2 實施型態中的資料處理裝置相同。

變形例中的資料處理裝置的加密裝置 27 具有如第 17 圖所示的結構。此加密裝置 27 包括第一解產生部 274X 和第二解產生部 274Y 這兩個解產生部，此點和只包括一個解產生部 274 的第 2 實施型態的資料處理裝置的加密裝置 27 不同。

第一解產生部 274X 和第二解產生部 274Y 皆以和第 2 實施型態中的解產生部 274 同樣的方式來產生解。

第一解產生部 274X 從介面部 271，以介面部 271 接收

了處理目標資料這個資訊為運作機會，以產生解。不過，第一解產生部 274X 亦可在每一次處理目標資料在前處理部 272 被分割時產生解。在第一解產生部 274X 上所產生的解被傳送至第一演算法產生部 275X 及第一密鑰產生部 276X。接收該解的第一演算法產生部 275X 及第一密鑰產生部 276X 分別以和第 2 實施型態相同的方式產生演算法和密鑰，再將其傳送至加密解密部 273。加密解密部 273 使用從第一演算法產生部 275X 及第一密鑰產生部 276X 所接收的演算法和密鑰，進行解密處理。

另一方面，第二解產生部 274Y 以介面部 271 接收了加密資料這個資訊為運作機會，以產生解。不過，第二解產生部 274Y 亦可在每一次加密資料在前處理部 272 被分割時產生解。在第二解產生部 274Y 上所產生的解被傳送至第二演算法產生部 275Y 及第二密鑰產生部 276Y。接收該解的第二演算法產生部 275Y 及第二密鑰產生部 276Y 分別以和第 2 實施型態相同的方式產生演算法和密鑰，再將其傳送至加密解密部 273。加密解密部 273 使用從第二演算法產生部 275Y 及第二密鑰產生部 276Y 所接收的演算法和密鑰，進行解密處理。

此外，第二解產生部 274Y 所產生的解相較於以相同順序所產生的解，同於第一解產生部 274X 所產生的解。此點同於，若比較以相同順序所產生的解，第 1 實施型態中的第一資料處理裝置 11 中所內建的加密裝置 27 內的解產生部 271 和第二資料處理裝置 12 中所內建的加密裝置 27A 內

的解產生部 271A 產生相同的解。亦即，此變形例中的第二解產生部 274Y 和第一解產生部 274X 具有相同解產生用演算法，而且，具有相同的初始陣列。

除了解的產生及演算法的產生的處理外，此變形例中的資料處理裝置執行和第 2 實施型態的資料處理裝置相同的處理。

此外，第 2 實施型態及其變形例所具有的加密裝置可置換成第 1 實施型態中的加密裝置 27B。

【圖式簡單說明】

第1圖圖示第1實施型態之資料處理系統的整體結構。

第2圖圖示第1圖所示之資料處理系統所包含之第一資料處理裝置的硬體結構。

第3圖為顯示第2圖所示之第一資料處理裝置所包含之通訊裝置之結構的方塊圖。

第4圖為顯示第2圖所示之第一資料處理裝置所包含之加密裝置之結構的方塊圖。

第 5 圖圖示第 1 圖所示之資料處理系統所包含之第二資料處理裝置的硬體結構。

第 6 圖為顯示第 5 圖所示之第二資料處理裝置所包含之加密裝置之結構的方塊圖。

第 7 圖為顯示第 5 圖所示之第二資料處理裝置所包含之其他加密裝置之結構的方塊圖。

第 8 圖為顯示第 5 圖所示之第二資料處理裝置所包含

之通訊裝置之結構的方塊圖。

第 9 圖為顯示在第 1 圖所示之資料處理系統上所執行之處理流程的流程圖。

第 10 圖為顯示在第 9 圖所示之 S110 中所執行之處理流程的流程圖。

第 11 圖為顯示在第 9 圖所示之 S130 中所執行之處理流程的流程圖。

第 12 圖為顯示在第 9 圖所示之 S140 中所執行之處理流程的流程圖。

第 13 圖為顯示在第 9 圖所示之 S150 中所執行之處理流程的流程圖。

第 14 圖圖示第 2 實施型態之資料處理裝置所包含之加密裝置的硬體結構。

第 15 圖為顯示在第 2 實施型態之資料處理裝置上所執行之加密處理流程的流程圖。

第 16 圖為顯示在第 2 實施型態之資料處理裝置上所執行之解密處理流程的流程圖。

第 17 圖圖示根據第 2 實施型態之資料處理裝置所作的變形例中所包含的加密裝置的硬體結構。

【主要元件符號說明】

11 第一資料處理裝置

12 第二資料處理裝置

13 網路

21 CPU

22 ROM

23 HDD

24 RAM

25 輸入裝置

26 顯示裝置

27, 27A, 27B 加密裝置

28 通訊裝置

29 匯流排

271, 271A, 271B 介面部

272, 272A, 272B 前處理部

273, 273A, 273B 加密解密部

274, 274A, 274B 解產生部

274X 第一解產生部

274Y 第二解產生部

275, 275A, 275B 演算法產生部

275X 第一演算法產生部

275Y 第二演算法產生部

276, 276A, 276B 密鑰產生部

276X 第一密鑰產生部

276Y 第二密鑰產生部

277, 277A, 277B 連接部

278B 選定資訊產生部

281 IF

282 認證資料產生部

283 通訊部

284 認證部

十、申請專利範圍：

102年4月8日修正本

1.一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於包括：

解產生裝置，將過去的解代入既定的解產生用演算法，以於既定的時序依次產生新解，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解演算法產生裝置，使用所產生的解在既定的時序中依次產生新演算法；以及

選定資訊記錄裝置，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；

其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

2.一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於包括：

解產生裝置，將過去的解代入既定的解產生用演算法，以於既定的時序依次產生新解，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解；

密鑰產生裝置，使用所產生的解在既定的時序中依次產生新密鑰；以及

選定資訊記錄裝置，將用來選定加密上述處理目標資料時所使用之上述密鑰的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；

其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

3.如申請專利範圍第1或2項之資料處理裝置，其中，包括一分割裝置，其可每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，將該加密資料分割為複數份加密分割資料，其分割係每隔和加密上述加密資料時所分割成之位元數相同的位元數進行，

其中，上述加密裝置在上述分割裝置上所分割的每個上述純文字分割資料上加密上述處理目標資料，以使之成為加密分割資料，

並且，上述解密裝置在每個上述加密分割資料上解密上述加密資料以使之成為純文字分割資料，另外又包括一連接裝置，其連接在上述加密裝置所加密的複數份上述加密分割資料以使之成為連貫的加密資料，並且，連接上述

解密裝置所解密的複數份上述純文字分割資料以使之成為連貫的處理目標資料。

4.如申請專利範圍第3項之資料處理裝置，其中，上述演算法產生裝置在每當進行上述處理目標資料的加密時，就產生上述演算法。

5.如申請專利範圍第3項之資料處理裝置，其中，上述演算法產生裝置在每當上述純文字分割資料被加密時，就產生上述演算法。

6.如申請專利範圍第1或2項之資料處理裝置，其中，上述解產生裝置將過去的複數個解代入上述解產生用演算法，得到上述解。

7.如申請專利範圍第1或2項之資料處理裝置，其中，上述解產生裝置在一開始產生上述解時，保留被代入上述解產生用演算法的初始解。

8.如申請專利範圍第3項之資料處理裝置，其中，上述密鑰產生裝置在每當進行上述處理目標資料的加密時，就產生上述密鑰。

9.如申請專利範圍第8項之資料處理裝置，其中，上述密鑰產生裝置在每當上述純文字分割資料被加密時，就產生上述密鑰。

10.如申請專利範圍第1項之資料處理裝置，其中，上述選定資訊為上述演算法。

11.如申請專利範圍第1項之資料處理裝置，其中，上述選定資訊為上述演算法產生裝置在產生上述演算法時所

使用的上述解。

12.如申請專利範圍第1項之資料處理裝置，其中，上述選定資訊表示下述資訊：上述演算法產生裝置在產生上述演算法時所使用的上述解，係為第幾個產生的解。

13.如申請專利範圍第2項之資料處理裝置，其中，上述選定資訊為上述密鑰。

14.如申請專利範圍第2項之資料處理裝置，其中，上述選定資訊為上述密鑰產生裝置在產生上述密鑰時所使用的上述解。

15.如申請專利範圍第2項之資料處理裝置，其中，上述選定資訊表示下述資訊：上述密鑰產生裝置在產生上述密鑰時所使用的上述解，係為第幾個產生的解。

16.一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，

其特徵在於包括：

解產生裝置，將過去的解代入既定的解產生用演算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，每進行一次上述處理目

標資料的加密，就依次產生新解；

第一演算法產生裝置，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；以及

第二演算法產生裝置產生新的演算法，其係與當使用所產生的解進行該加密資料的解密時，由上述第一演算法產生裝置依序產生的演算法相同；

其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

17.一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，

其特徵在於包括：

第一解產生裝置，將過去的解代入既定的解產生用演算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一演算法產生裝置，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；

第二解產生裝置，將過去的解代入既定的解產生用演算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；以及

第二演算法產生裝置產生新的演算法，其係與當使用上述第二解產生裝置所產生的解進行該加密資料的解密時，由上述第一演算法產生裝置依序產生的演算法相同；

其中，上述第一解產生裝置及第二解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

18. 一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，

其特徵在於包括：

解產生裝置，將過去的解代入既定的解產生用演算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一密鑰產生裝置，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；以及

第二密鑰產生裝置產生新的密鑰，其係與當使用所產生的解進行該加密資料的解密時，由上述第一密鑰產生裝置依序產生的密鑰相同；

其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

19.一種資料處理裝置，包括使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的加密裝置、記錄該加密資料的記錄裝置、及解密裝置，其中該解密裝置將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰，其加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密，

其特徵在於包括：

第一解產生裝置，將過去的解代入既定的解產生用演算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一密鑰產生裝置，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；

第二解產生裝置，將過去的解代入既定的解產生用演

算法，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生裝置上依次產生的解相同的新解；以及

第二密鑰產生裝置產生新的密鑰，其係與當使用上述第二解產生裝置所產生的解進行該加密資料的解密時，由上述第一密鑰產生裝置依序產生的密鑰相同；

其中，上述第一解產生裝置及第二解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

20.如申請專利範圍第16至19項中任一項之資料處理裝置，其中，包括一分割裝置，其可每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，將該加密資料分割為複數份加密分割資料，其分割係每隔和加密上述加密資料時所分割成之位元數相同的位元數進行，

上述加密裝置在上述分割裝置上所分割的每個上述純文字分割資料上加密上述處理目標資料，以使之成為加密分割資料，並且，上述解密裝置在每個上述加密分割資料上解密上述加密資料以使之成為純文字分割資料，

另外又包括一連接裝置，其連接在上述加密裝置所加密的複數份上述加密分割資料以使之成為連貫的加密資料，並且，連接上述解密裝置所解密的複數份上述純文字分割資料以使之成為連貫的處理目標資料。

21.一種資料處理系統，其結構包含複數個第一資料處理裝置、相同數目且與各個上述第一資料處理裝置對應的第二資料處理裝置及第三資料處理裝置，

在上述第一資料處理裝置和上述第二資料處理裝置之間，進行純文字處理目標資料加密後的加密資料的通訊，並且，在上述第二資料處理裝置和上述第三資料處理裝置之間，進行處理目標資料上的通訊，

其特徵在於：

上述第一資料處理裝置和上述第二資料處理裝置皆包括：

分割裝置，每隔既定的位元數分割上述處理目標資料以使之成為複數份純文字分割資料，並且，將該加密資料分割為複數份加密分割資料，其分割係每隔和加密上述加密資料時所分割成之位元數相同的位元數進行；

解產生裝置，依次產生在對應之上述第一資料處理裝置和上述第二資料處理裝置上為共用且和其他上述第一資料處理裝置和上述第二資料處理裝置不同的解；

加密解密裝置，將該純文字分割資料加密使之成為加密分割資料，其係藉由根據從上述解產生裝置接收之上述解所產生之該第一資料處理裝置和該第二資料處理裝置上共用的演算法進行，並且，將該加密分割資料解密成為純文字分割資料，其係藉由將該加密分割資料加密時使用的演算法進行；以及

連接裝置，連接解密後的上述純文字分割資料以使之

成為上述處理目標資料；

收發裝置，收發上述加密資料；

並且，上述第三資料處理裝置為申請專利範圍第1至20項中任一項之資料處理裝置，將處理目標資料加密，其中該處理目標資料為，上述第二資料處理裝置將上述第一資料處理裝置所加密的加密資料予以解密，所產生的處理目標資料，，並將該加密資料記錄於上述記錄裝置，並且，解密從該記錄裝置讀取的加密資料，將之傳送至上述第二資料處理裝置。

22.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料的步驟，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於：

上述資料處理裝置執行：

步驟一，將過去的解代入既定的解產生用演算法，以於既定的時序依次產生新解，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解；

步驟二，使用所產生的解在既定的時序中依次產生新演算法；以及

步驟三，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既

定的記錄裝置上；

其中，上述解產生裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

23.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料的步驟，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於：

上述資料處理裝置執行：

步驟一，將過去的解代入既定的解產生用演算法，以於既定的時序依次產生新解，其中該既定的解產生用演算法係能夠藉由代入至少一個過去的解來產生新的解；

步驟二，使用所產生的解在既定的時序中依次產生新密鑰；以及

步驟三，將用來選定加密上述處理目標資料時所使用之上述演算法的選定資訊和上述加密資料關聯，記錄於既定的記錄裝置上；

其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解。

24.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝

置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料的步驟，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於：

上述資料處理裝置執行：

將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法的步驟，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一演算法產生步驟，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；以及

第二演算法產生步驟，產生新的演算法，其係與當使用所產生的解進行該加密資料的解密時，由上述第一演算法產生步驟中依序產生的演算法相同；

其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

25.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料的步驟，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於：

上述資料處理裝置執行：

第一解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一演算法產生步驟，使用在上述第一解產生裝置上所產生的解在每次進行上述處理目標資料的加密時依次產生新演算法；

第二解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生步驟上依次產生的解相同的新解；以及

第二演算法產生步驟，產生新的演算法，其係與當使用第二解產生步驟中所產生的解進行該加密資料的解密時，由上述第一演算法產生步驟中依序產生的演算法相同；

其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

26.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝

置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料，其係使用將該加密資料加密時所使用的演算法以及密鑰的步驟，

其特徵在於：

上述資料處理裝置執行：

將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解的步驟；

第一密鑰產生步驟，使用所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；以及

第二密鑰產生步驟，產生新的密鑰，其係與當使用所產生的解進行該加密資料的解密時，由上述第一密鑰產生步驟中依序產生的密鑰相同；

其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。

27.一種資料處理方法，在資料處理裝置上執行使用既定的演算法及既定的密鑰加密純文字處理目標資料以使之成為加密資料的步驟、將該加密資料記錄於既定的記錄裝置的步驟、將從該記錄裝置讀出的加密資料解密使之成為處理目標資料的步驟，其係使用將該加密資料加密時所使用的演算法以及密鑰，

其特徵在於：

上述資料處理裝置執行：

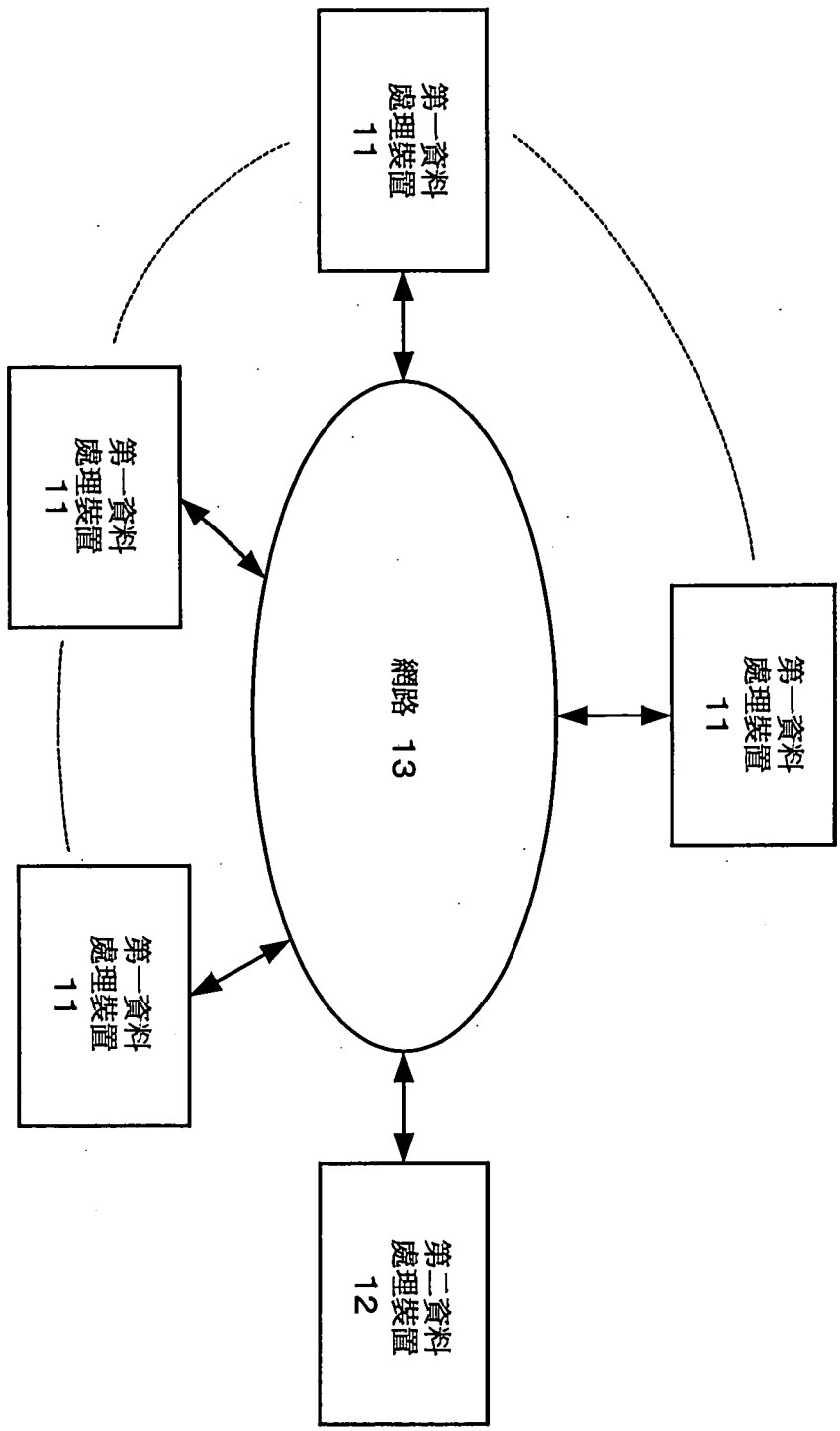
第一解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，每進行一次上述處理目標資料的加密，就依次產生新解；

第一密鑰產生步驟，使用在上述第一解產生步驟上所產生的解在每次進行上述處理目標資料的加密時依次產生新密鑰；

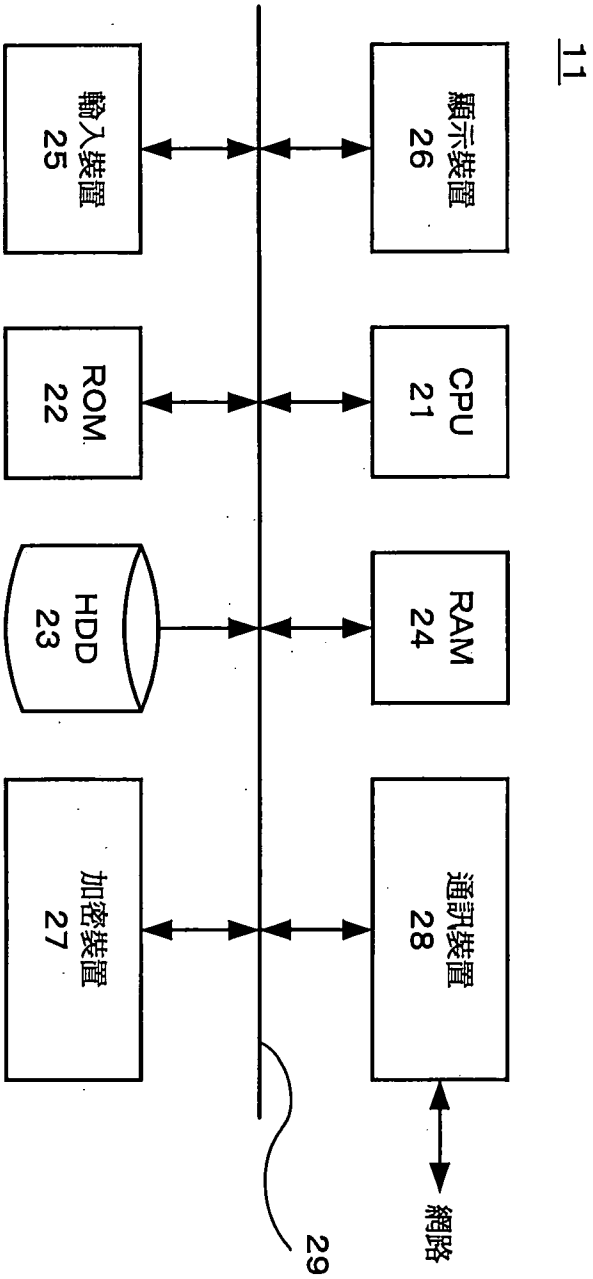
第二解產生步驟，將過去的解代入可藉由代入過去的解中的至少其中一個來產生新解的既定解產生用演算法，藉此，產生與每次進行上述加密資料的解密時在上述第一解產生步驟上依次產生的解相同的新解；以及

第二密鑰產生步驟，產生新的密鑰，其係與當使用上述第二解產生步驟所產生的解進行該加密資料的解密時，由上述第一密鑰產生步驟中依序產生的密鑰相同；

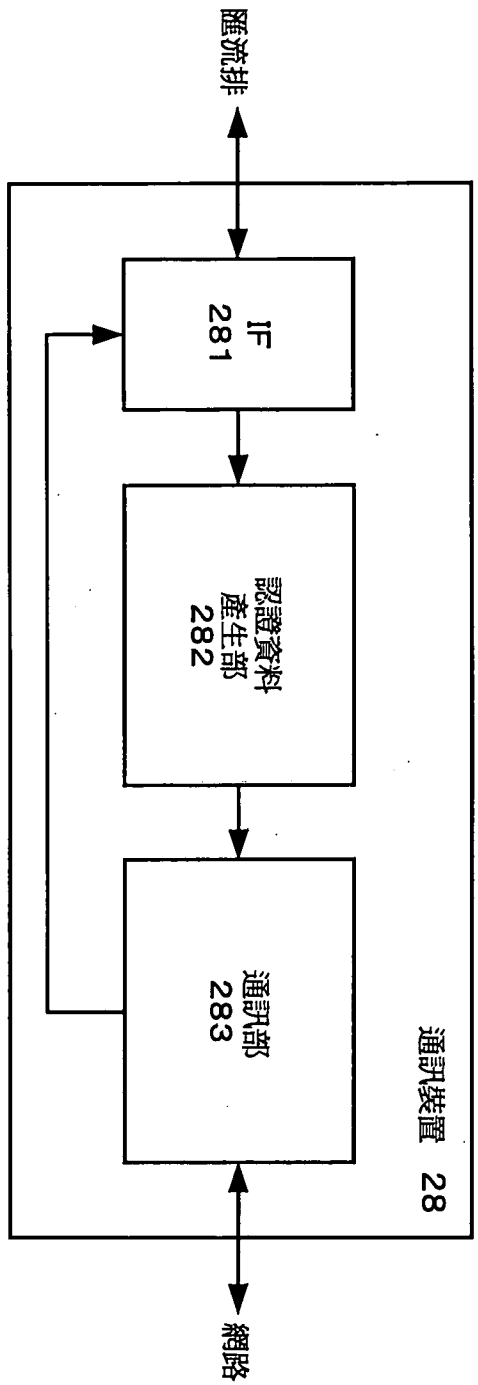
其中，上述資料處理裝置保留過去的解的至少其中一個，並且，在不需要重新代入的時點，刪除過去的解，另外，加密複數份處理目標資料以使之成為加密資料，並且，使用和加密複數份上述加密資料時相同的順序對其進行解密。


第一資料處理裝置 11
第一資料處理裝置 11
第一資料處理裝置 11
第一資料處理裝置 11
網路 13
第二資料處理裝置 12

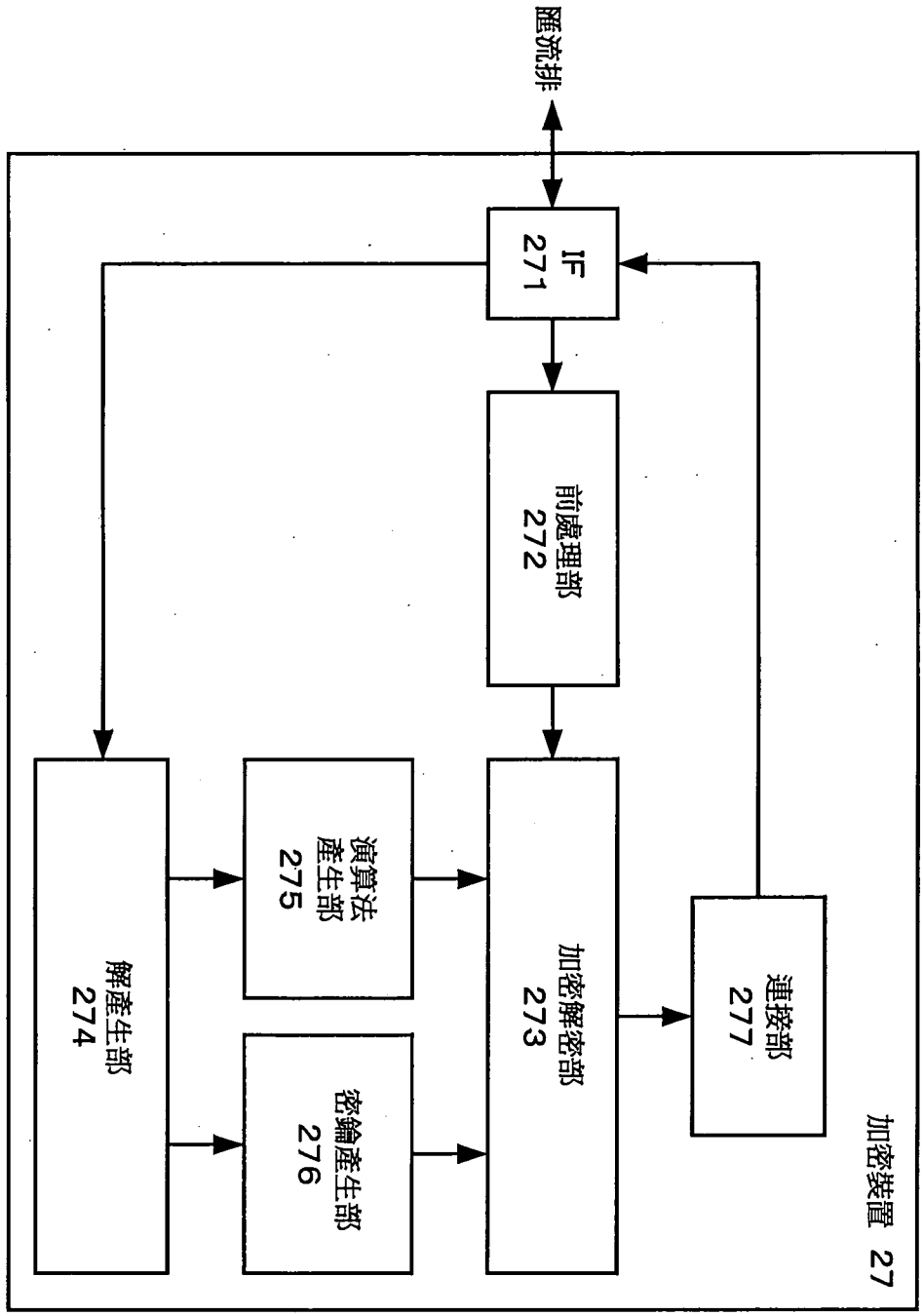
第1圖


11
顯示裝置
26
輸入裝置
25
CPU
21
ROM
22
RAM
24
HDD
23
通訊裝置
28
加密裝置
27
網路
29

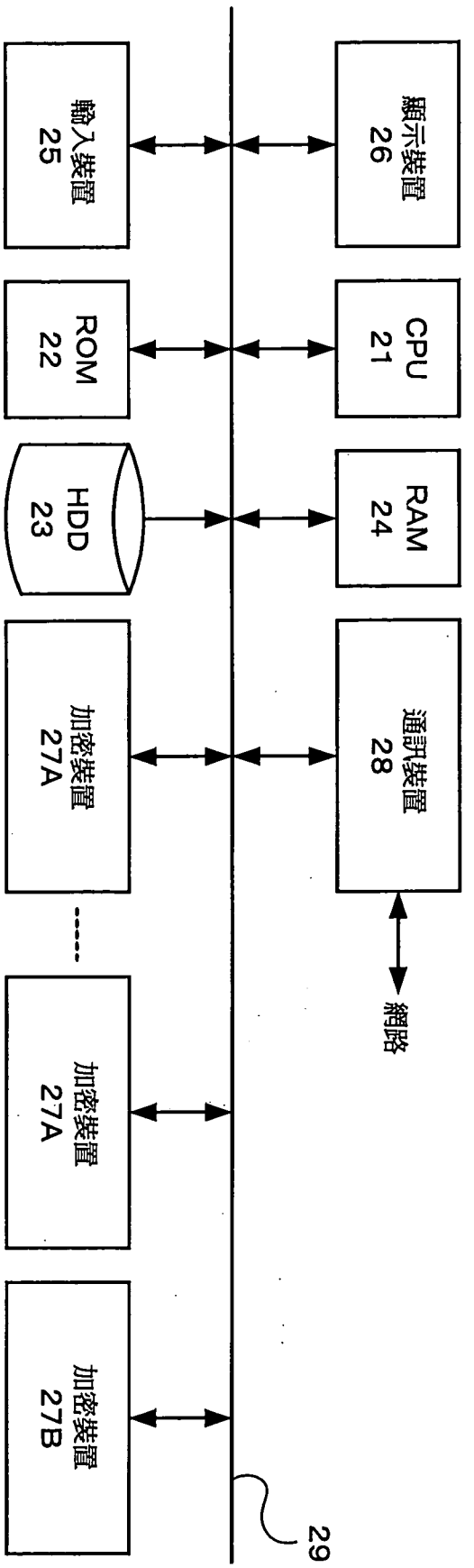
第2圖



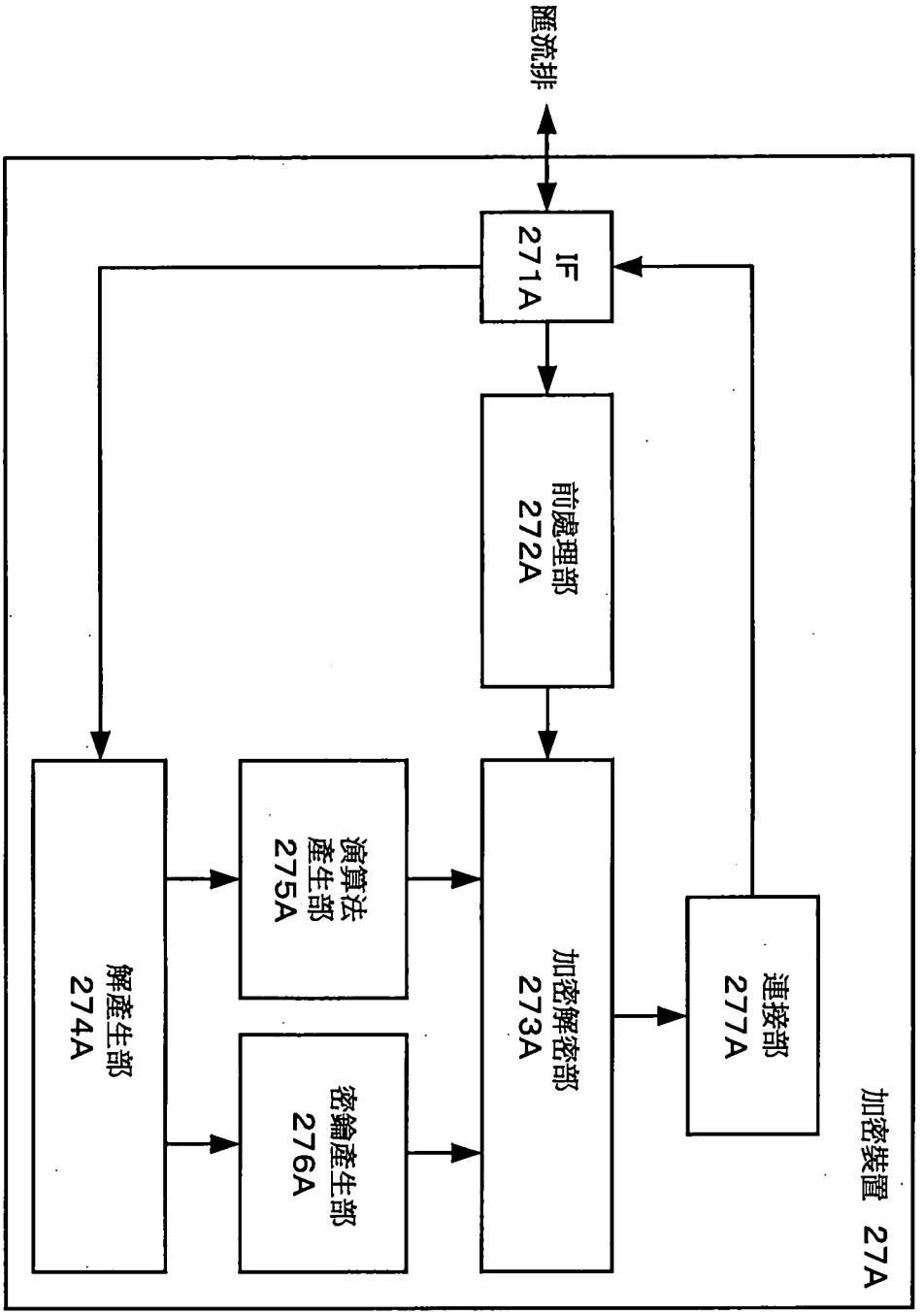
第3圖


匯流排
IF
271
前處理部
272
加密解密部
273
連接部
277
加密裝置 27
演算法
產生部
275
密鑰產生部
276
解產生部
274

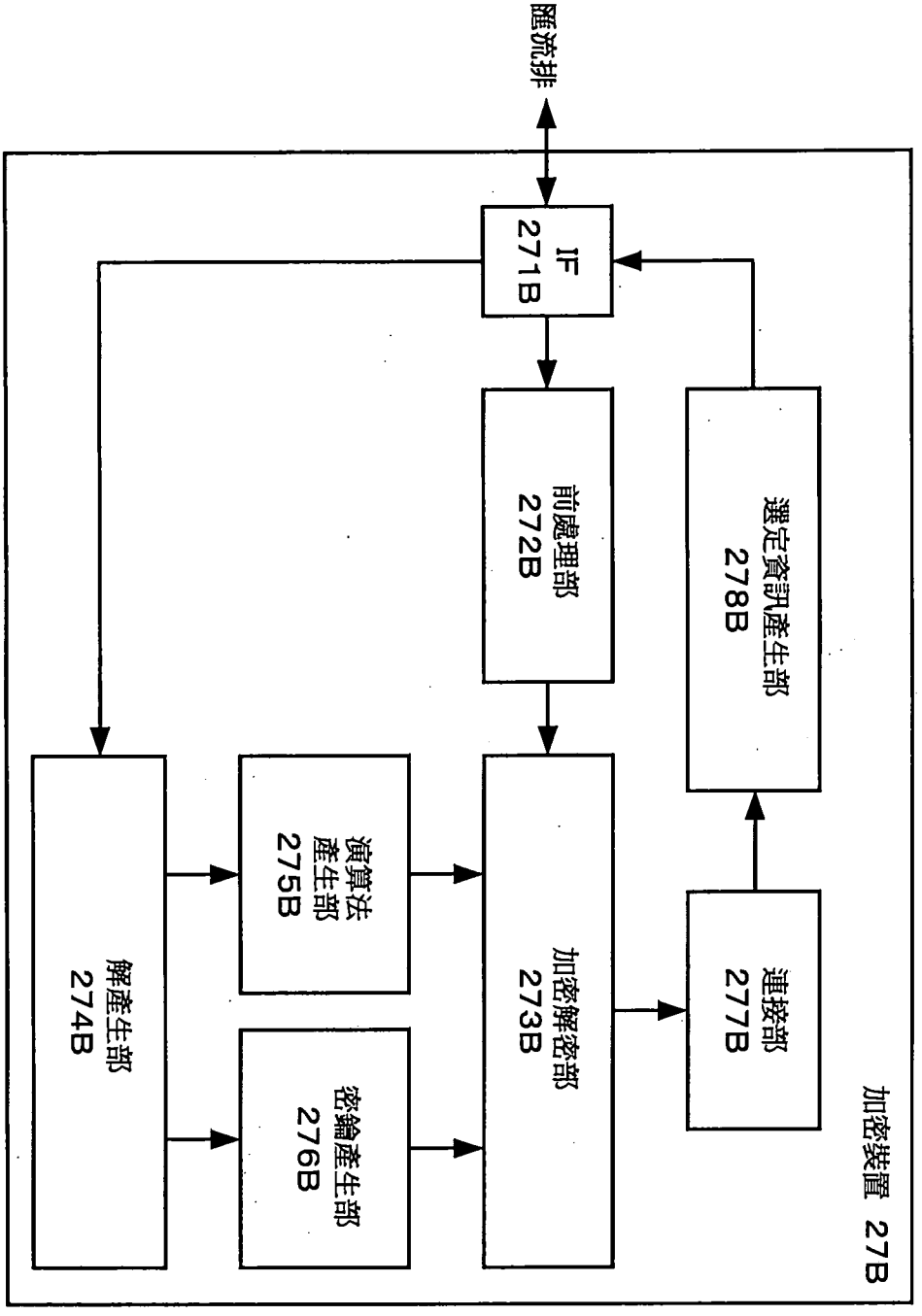
第4圖


12
顯示裝置
26
輸入裝置
25
CPU
21
ROM
22
RAM
24
HDD
23
通訊裝置
28
加密裝置
27A
加密裝置
27A
加密裝置
27B
網路
29

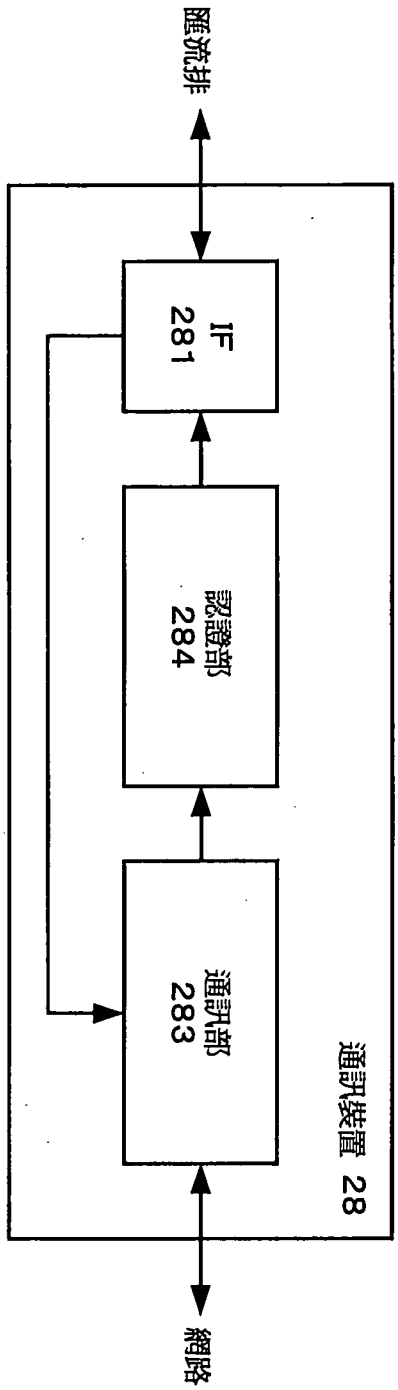
第5圖


匯流排
IF
271A
前處理部
272A
加密解密部
273A
連接部
277A
演算法
產生部
275A
密鑰產生部
276A
解產生部
274A
加密裝置 27A

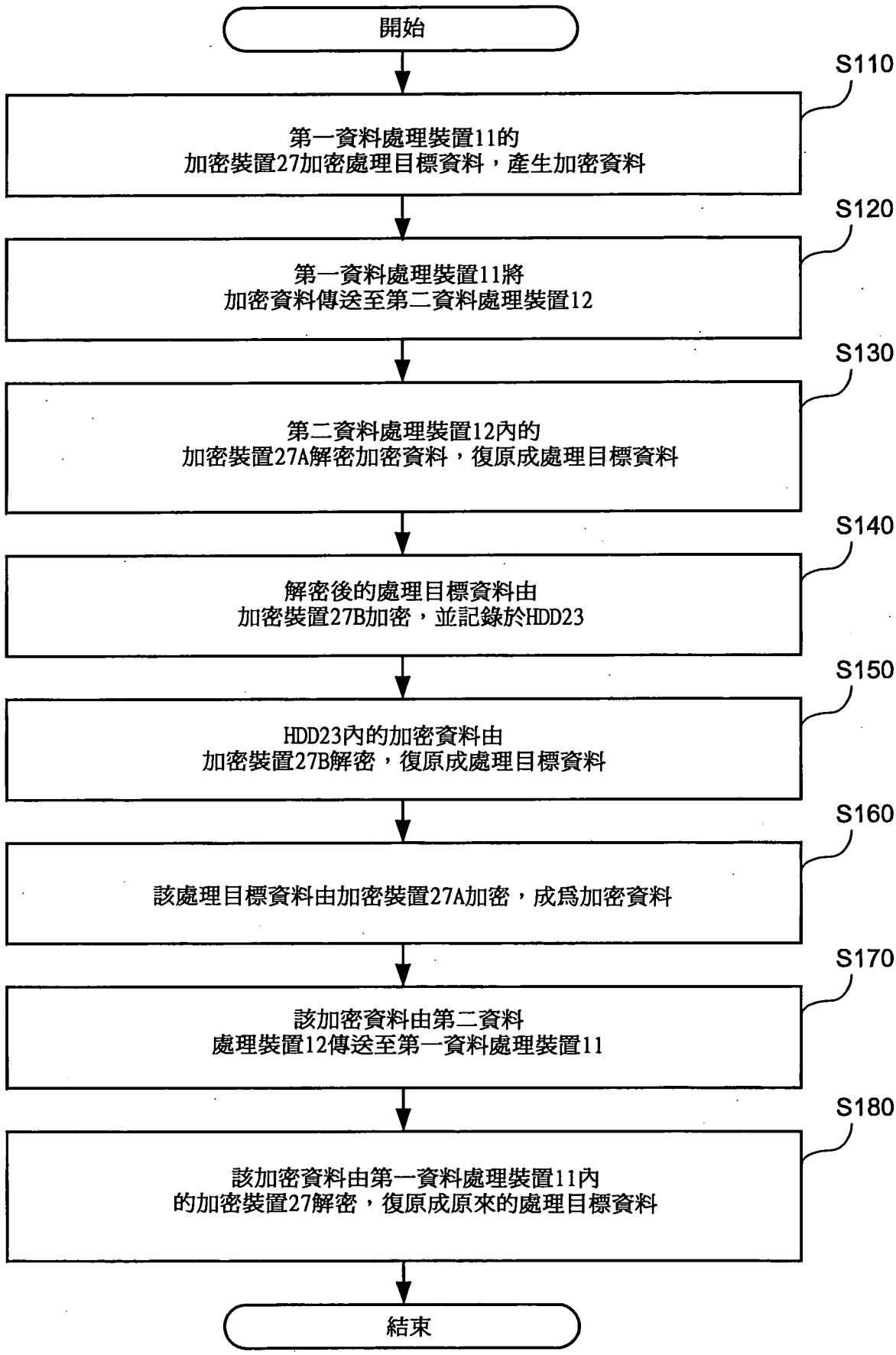
第6圖


匯流排
IF
271B
前處理部
272B
選定資訊產生部
278B
加密解密部
273B
連接部
277B
演算法
產生部
275B
密鑰產生部
276B
解產生部
274B
加密裝置 27B

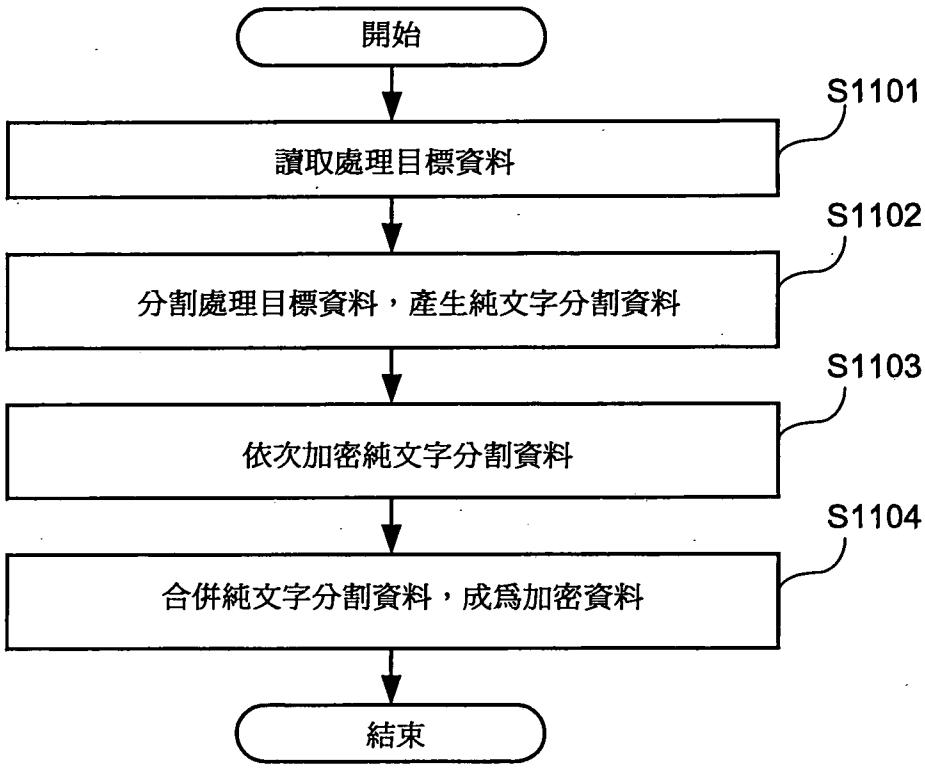
第7圖



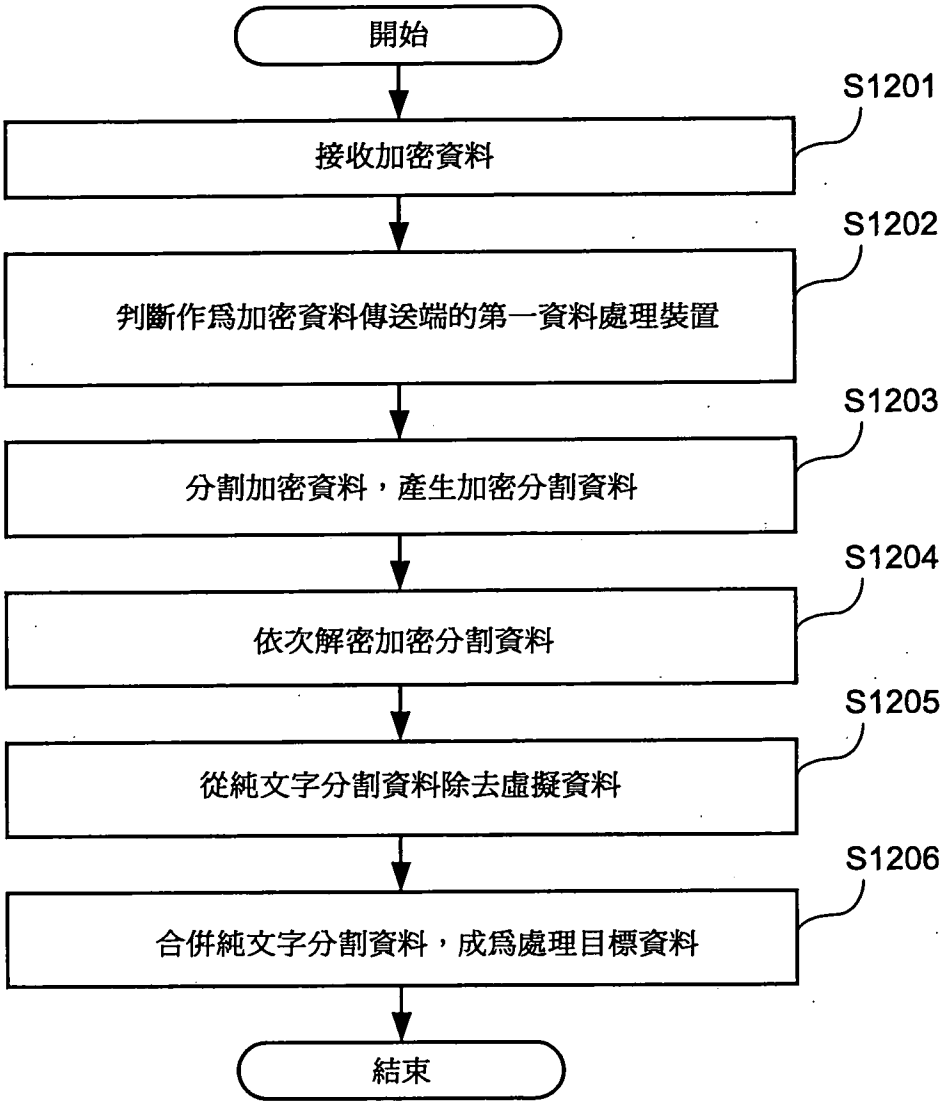
第8圖


開始
S110
第一資料處理裝置11的
加密裝置27加密處理目標資料，產生加密資料
S120
第一資料處理裝置11將
加密資料傳送至第二資料處理裝置12
S130
第二資料處理裝置12內的
加密裝置27A解密加密資料，復原成處理目標資料
S140
解密後的處理目標資料由
加密裝置27B加密，並記錄於HDD23
S150
HDD23內的加密資料由
加密裝置27B解密，復原成處理目標資料
S160
該處理目標資料由加密裝置27A加密，成爲加密資料
S170
該加密資料由第二資料
處理裝置12傳送至第一資料處理裝置11
S180
該加密資料由第一資料處理裝置11內
的加密裝置27解密，復原成原來的處理目標資料
結束

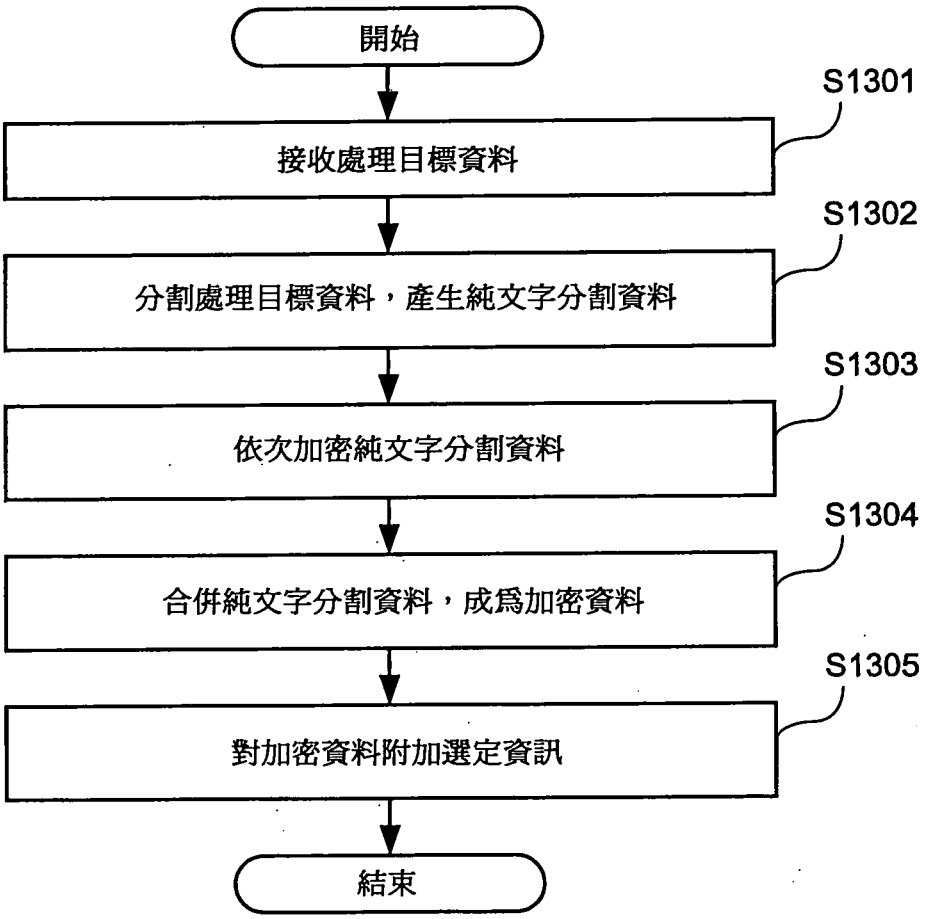
第9圖


開始
S1101
讀取處理目標資料
S1102
分割處理目標資料，產生純文字分割資料
S1103
依次加密純文字分割資料
S1104
合併純文字分割資料，成爲加密資料
結束

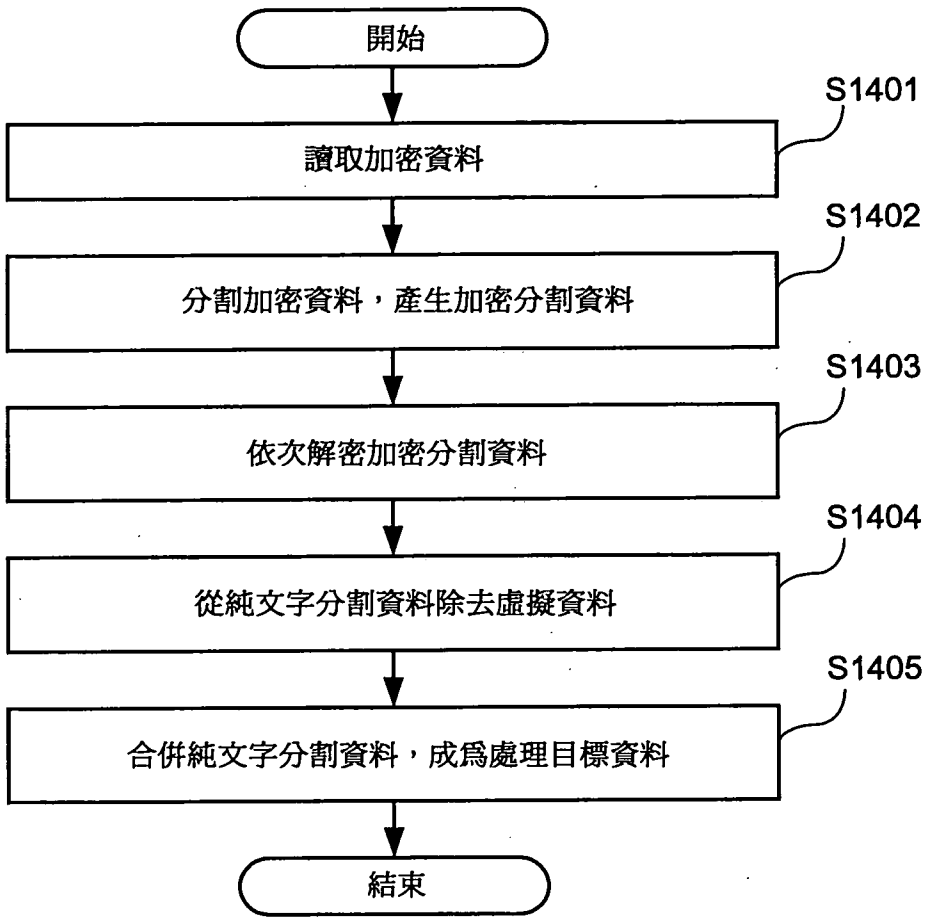
第10圖


開始
S1201
接收加密資料
S1202
判斷作爲加密資料傳送端的第一資料處理裝置
S1203
分割加密資料，產生加密分割資料
S1204
依次解密加密分割資料
S1205
從純文字分割資料除去虛擬資料
S1206
合併純文字分割資料，成爲處理目標資料
結束

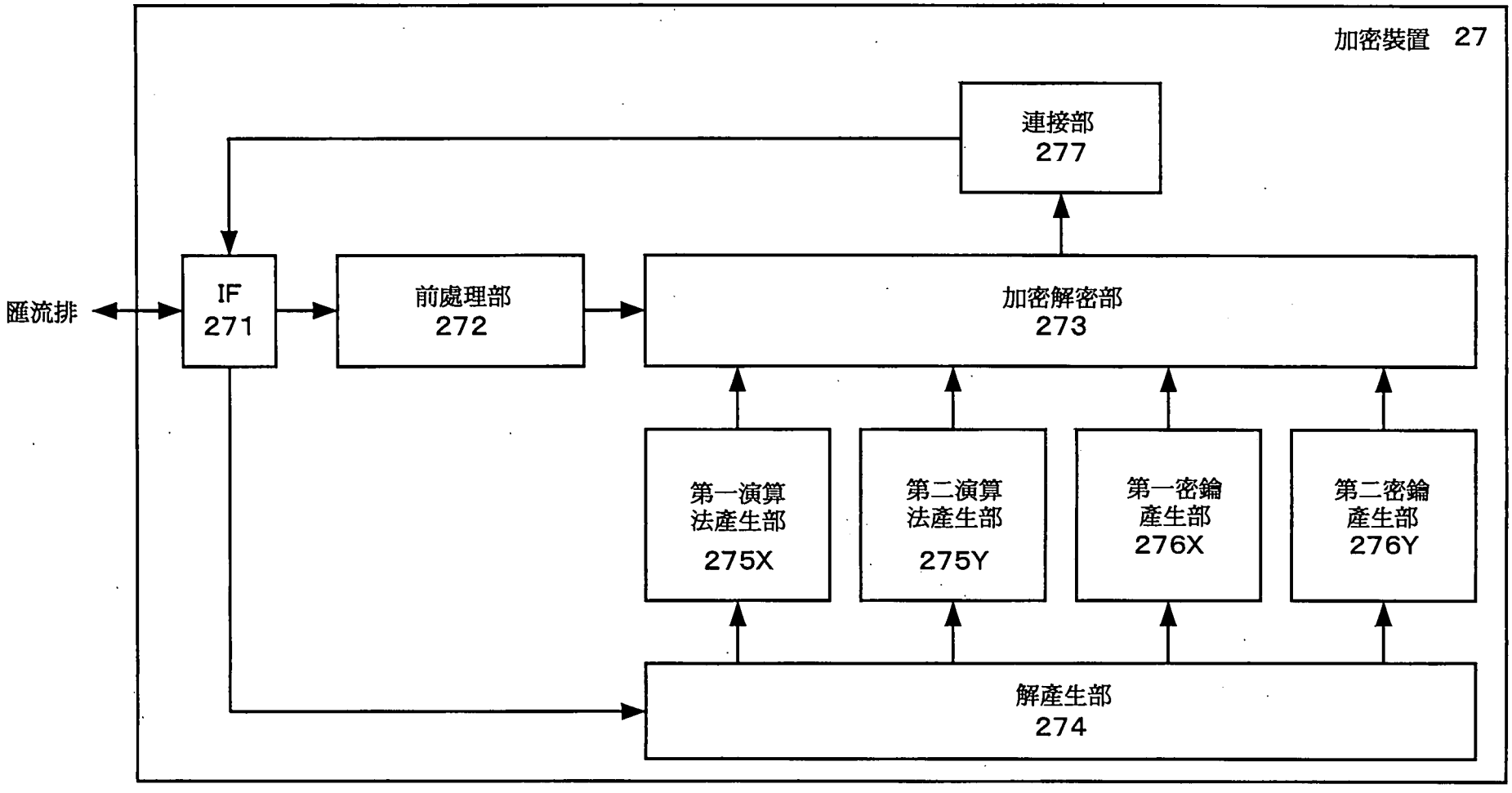
第11圖


開始
S1301
接收處理目標資料
S1302
分割處理目標資料，產生純文字分割資料
S1303
依次加密純文字分割資料
S1304
合併純文字分割資料，成爲加密資料
S1305
對加密資料附加選定資訊
結束

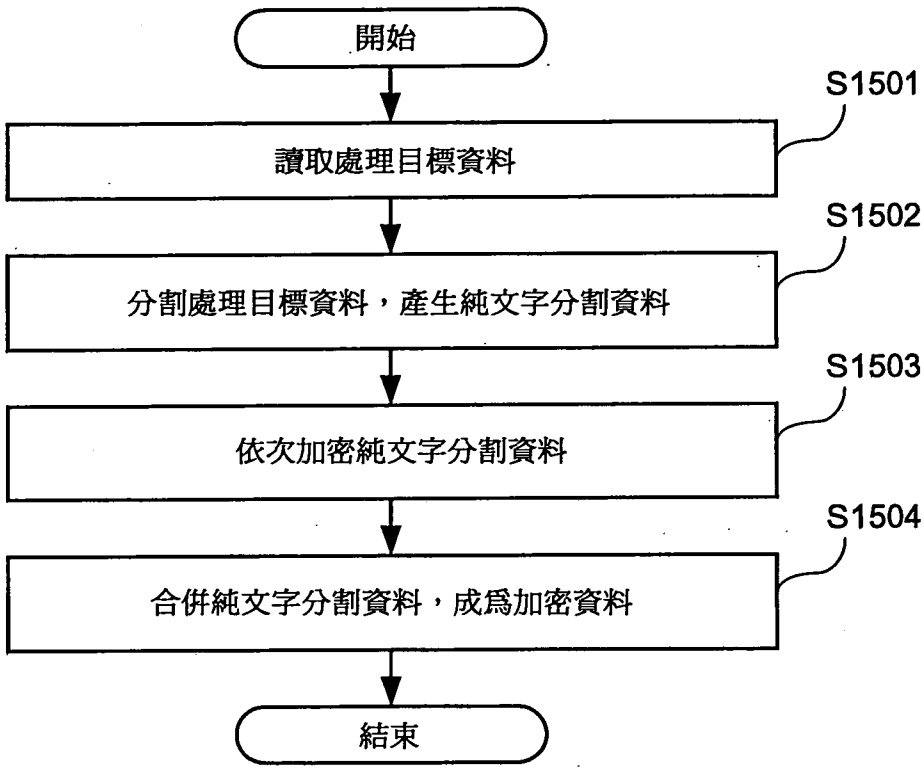
第12圖


開始
S1401
讀取加密資料
S1402
分割加密資料，產生加密分割資料
S1403
依次解密加密分割資料
S1404
從純文字分割資料除去虛擬資料
S1405
合併純文字分割資料，成爲處理目標資料
結束

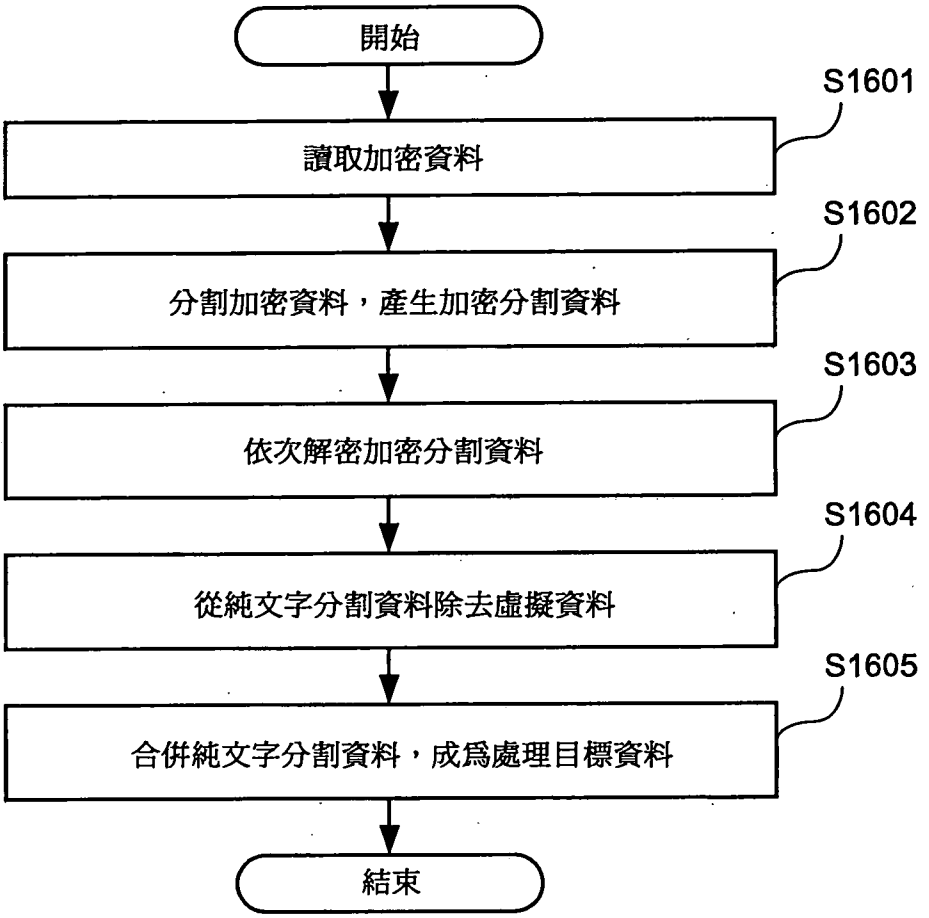
第13圖


加密裝置 27
連接部
277
匯流排
IF
271
前處理部
272
加密解密部
273
第一演算
法產生部
275X
第二演算
法產生部
275Y
第一密鑰
產生部
276X
第二密鑰
產生部
276Y
解產生部
274

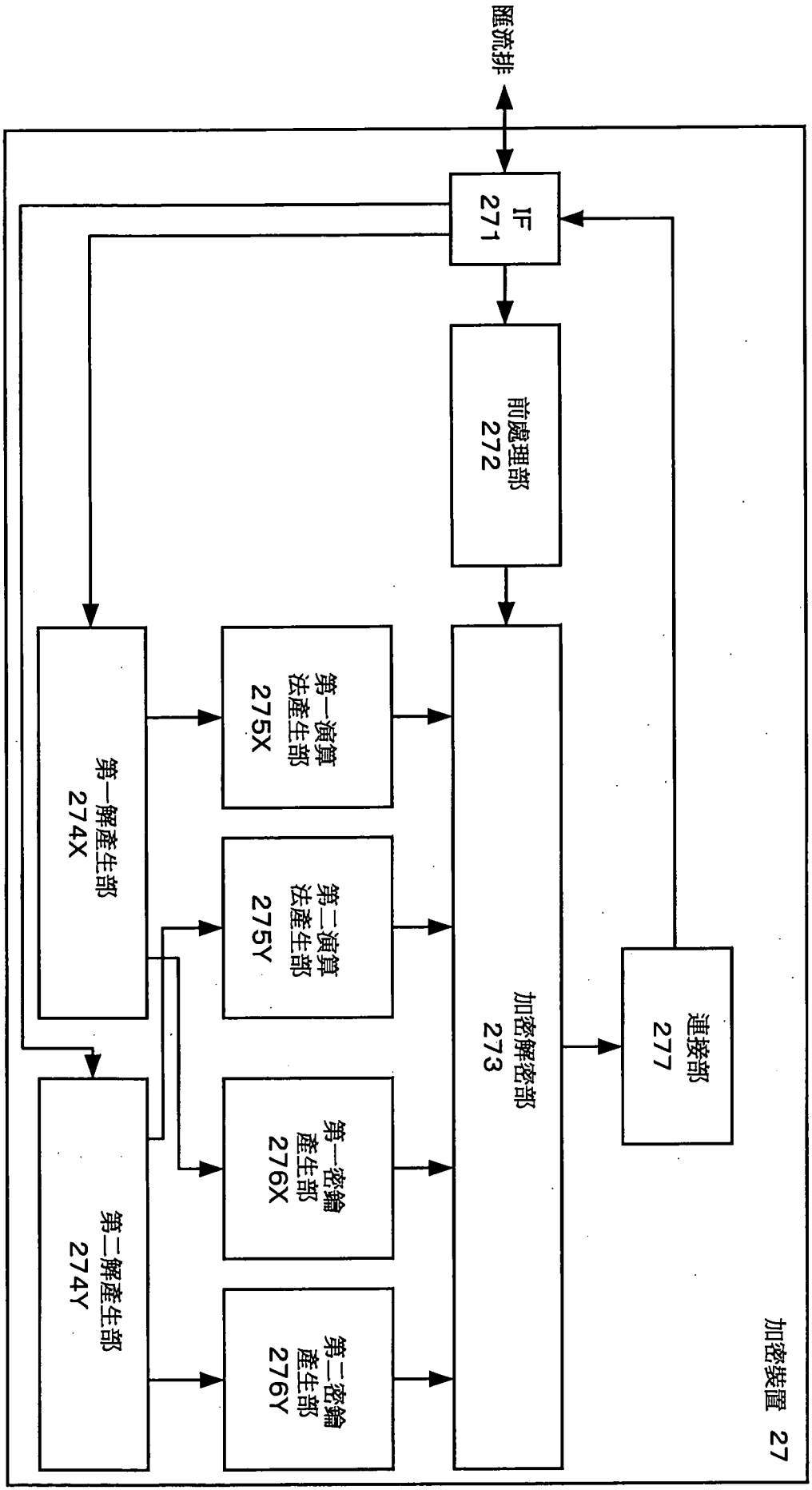
第14圖


開始
S1501
讀取處理目標資料
S1502
分割處理目標資料，產生純文字分割資料
S1503
依次加密純文字分割資料
S1504
合併純文字分割資料，成爲加密資料
結束

第15圖


開始
S1601
讀取加密資料
S1602
分割加密資料，產生加密分割資料
S1603
依次解密加密分割資料
S1604
從純文字分割資料除去虛擬資料
S1605
合併純文字分割資料，成爲處理目標資料
結束

第16圖


匯流排
IF
271
前處理部
272
加密解密部
273
連接部
277
加密裝置 27
第一演算
法產生部
275X
第二演算
法產生部
275Y
第一解產生部
274X
第二解產生部
274Y
第一密鑰
產生部
276X
第二密鑰
產生部
276Y

第17圖