I307593

公告本

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：94144329

※申請日期 94.12.14 ※IPC分類： H04L 9/00, G06F12/1

一、發明名稱：（中文/英文） (2006.01)

保護數位資料之系統及其方法

SYSTEM AND METHOD OF PROTECTING DIGITAL DATA

二、申請人：（共 1 人）

姓名或名稱 （中文/英文）

國防部軍備局中山科學研究院

CHUNG SHAN INSTITUTE OF SCIENCE AND TECHNOLOGY

代表人 （中文/英文）

龔家政 / KUNG, CHIA CHENG

住居所或營業所地址： （中文/英文）

桃園縣龍潭鄉佳安村6鄰中正路佳安段481號

No.481, Jia-an Sec., Jhongjheng Rd., Longtan Township, Taoyuan County , Taiwan, R.O.C.

國籍： （中文/英文）

中華民國 / Taiwan, R.O.C.

三、發明人：（共 4 人）

姓 名：（中文/英文）

陳彥甫 / CHEN, YEN FU

王宣斯 / WANG, HSUAN SSU

楊益全 / YANG, I CHUAN

李國田 / LI, KUO TIEN

國　籍:　　（中文/英文）

中華民國　/　Taiwan, R.O.C.
中華民國　/　Taiwan, R.O.C.
中華民國　/　Taiwan, R.O.C.
中華民國　/　Taiwan, R.O.C.

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：

□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】

本發明係為一種保護數位資料之系統及其方法，特別係可在一對多傳送時，達到節省傳送端個人電腦傳輸頻寬以及安全控管之系統及其方法。

【先前技術】

隨著網際網路（Internet）的日益發達，由於簡單的操作介面以及方便的使用環境，使用者越來越習慣於利用網路來傳送文件，不僅能將文件快速的傳到對方手上，所花費之成本也較傳統郵寄方式來的低廉。但是這樣的方式很可能會被其他有心人從傳送過程中盜取，或者可能為伺服器本身設計之問題而被公開。這種網路上侵犯著作權的問題已經日益氾濫，為了解決諸如此類的問題，數位權證管理（DRM，Digital Rights Management）的相關技術便應運而生。

所謂的數位權證管理，主要是用來管制數位資訊在網路上的非法散佈，可以使得僅有獲得著作人授權的特定使用者，可以依據著作人原先所同意的使用範圍與期限來使用數位資訊，而未獲得授權的使用者則無法使用甚至無法存取數位資訊。

一般電子文件與數位資料保護做法，是將保護的電子文件產生一加密電子文件與該加密電子文件的解密金鑰兩部份，將加密電子文件傳送至使用者，並將該加密電子文件的解

密金鑰在資料庫內進行控管，再由使用者將取出加密電子文件的解密金鑰與加密電子文件進行解密作業。

但是，上述的數位權證管理軟體卻仍然可以讓未授權者下載加密的數位資訊，如果未授權者一旦對加密後的數位資訊成功解密，則數位資訊就如同未受到數位權證管理軟體的保護一般。

為了解決上述的問題，美國專利第 6,289,450 號以及美國專利第 6,339,825 號，便提出了設定資訊保密政策（policy）來保護數位資訊不被未授權者存取的方法，但是上述的各種數位資訊的保護方法仍有兩個缺點。

其一，當數位權證軟體在對數位資訊進行加密時，僅是利用簡單的單層加密方式，而且將解密的金鑰就放在加密後的數位資訊中。因此，有心人士便可能會利用一些特殊方式來找出解密金鑰的位置，而將加密後的數位資訊進行解密，取得被保護之資料。其二，如果數位資訊中未附加解密金鑰，使用者要使用或閱覽數位資訊，就必須要連線上網路以便線上即時取得解密所需的金鑰。

另一種做法是使用者透過伺服器，將加密保護檔案直接傳送至另一使用者，然後，此另一使用者可同時再向伺服器端索取加密保護檔案之解密金鑰，此系統適合在一對一傳輸方式下進行，若在經常性的一對多文件傳送上，並不恰當。目前一般作法是由使用者將加密保護檔案傳送至另一使用者，但除了

佔據網路頻寬外，增加資訊外洩的可能性，尤其目前有些資訊檔案需要更安全的集中保護管控，目前方法無法滿足需求，因此，提出一種新的管理方案來解決目前的問題。

【發明內容】

鑒於以上的問題，本發明的主要目的在於提供一種保護數位資料之系統及其方法，藉以二把金鑰及在伺服器集中控管加密文件，達成雙重安全防護及避免加密文件在外被相互傳送而增加被破解之風險，再者，當使用者欲傳送同一文件至多個接收端時，只需傳送金鑰至多個接收端之方式，可大大減少傳送者之頻寬負荷。

因此，為達上述目的，本發明所揭露之一種保護數位資料之系統，包含：傳送端、接收端以及伺服器。其中在傳送端包含：

編輯程式，用以編輯檔案內容，其中當檔案內容進行傳送到接收端時，會使用共同金鑰與檔案金鑰對於檔案內容進行兩層加密作業，並產生兩個加密檔案，其中第一個加密檔案為傳送至伺服器，包含一先以檔案金鑰進行檔案內容的第一層加密，再以共同金鑰進行第二層加密之第二加密電子文檔，一接收端下載權限清單以及接收端軟體功能關閉權限清單；而第二個加密檔案包含將檔案內容摘要與檔案金鑰以共同金鑰進行加密，並以電子郵件夾帶方式傳送至接收端。

然第一個加密檔案傳送至網際網路上之一伺服器，會依據

傳送端所設定接收端下載權限清單之權限，接收端依據此權限至伺服器下載資料庫中之第二加密電子文檔。

因此，在接收端包含：

解密模組，用以將先前所接收到之第二個加密檔案，以共同金鑰解密取出其中夾帶之檔案金鑰，以及檔案內容摘要，並將第二加密電子文檔解密成第一加密電子文檔；編輯程式，用以利用解密取得之檔案金鑰，並可將第一加密電子文檔解密，使用者因而得以開啟及閱讀檔案內容。

依據本發明之目的且達到上述之優點，本發明應用在傳送端進行保護數位資料之方法，包含下列步驟：

當使用者在編輯程式完成檔案內容編輯而欲傳送到接收端時，首先，以檔案金鑰將檔案內容加密成第一加密電子文檔，確認使用者輸入所要傳送的檔案及各接收端使用者之傳送指令？當使用者按下傳送鍵時，先由編輯程式擷取或輸入檔案內容摘要及檔案金鑰，並以共同金鑰一併加密成第二個加密檔案傳送至接收端；而第一加密電子文檔以共同金鑰進行第二次加密成第二加密電子文檔，確認是否加密完成？當完成後，則將第二加密電子文檔、接收端下載權限清單以及接收端軟體功能關閉權限清單，形成第一個加密檔案，一同傳送至伺服器傳送至網際網路上之一伺服器，並儲存於一資料庫。

本發明應用在接收端進行保護數位資料之方法，包含下列步驟：

首先，接收傳送端傳來之以共同金鑰加密過之第二個加密檔案，包含檔案內容摘要及檔案金鑰，編輯程式以共同金鑰可解讀檔案內容摘要，並獲取進入伺服器下載該檔案內容摘要對應之第二加密電子文檔；然後，以共同金鑰對第二加密電子文檔進行解密，確認解密工作是否完成？當解密成第一加密電子文檔時，在編輯程式中再確認是否可以先前所收到之檔案金鑰進行解密？當確認無誤後，即可以檔案金鑰還原成可開啟並閱讀之檔案內容。

有關本發明的特徵與實作，茲配合圖示作最佳實施例詳細說明如下。

【實施方式】

本發明將揭露一種保護數位資料之系統及其方法。在本發明的以下詳細說明中，將描述多種特定的細節以便提供本發明的完整說明。然而，對熟知技藝者來說，並可以不需要使用該等特定細節便可以實施本發明，或者可以藉著利用替代的元件或方法來實施本發明。在其他的狀況下，並不特別詳細地說明已知的方法、程序、部件、以及電路，以免不必要地混淆本發明的重點。

請參照「第 1a 圖」，此為傳送端 10 傳送檔案內容 110 至接收端 20 之系統架構示意圖，請一併參照「第 2a 圖」，此為傳送端 10 傳送檔案內容 110 至接收端 20 之方法流程圖。當傳送端 10 之使用者在編輯程式 100 編輯一檔案內容 110，而

準備傳至接收端 20 時(步驟 310)，首先，使用者可於編輯程式 100 中進行該檔案之編輯，當判斷使用者已經選擇進行檔案內容 110 傳送時(步驟 315)，會先以檔案金鑰 120 對檔案內容 110 進行 AES-256 加密(步驟 320)，也可利用其他的對稱式之加密方式，例如：DES、3-DES、RC5、及 IDEA…等。

在準備進行傳送的同時，也擷取檔案內容 110 之主旨、摘要及部分內容編成檔案內容摘要 170，再由加密模組 130 利用共同金鑰 150 對檔案內容摘要 170 以及檔案金鑰 120 進行加密成第一個加密檔案，可以透過編輯程式 100 中之傳檔程式，或是以電子郵件(e-mail)220 之方式來進行傳送，在加入該電子郵件 220 之附件中，經由網際網路 50 傳送到接收端 20(步驟 325)進行通知；此一共同金鑰 150 可以依不同群組來作設定，因此，即使在同一公司所使用之編輯程式 100 雖然皆相同，但是由於內部不同群組的編輯程式 100 所使用之共同金鑰 150 並不相同，因此即便文件被其他群組的使用者所獲取，也無法被開啟，藉此可達到避免被閒雜人等竊取窺視之風險。

而檔案內容 110 進行傳送的過程中，在經過編輯程式 100 以檔案金鑰 120 進行第一層加密而成第一加密電子文檔 140 後，再以共同金鑰 150，由加密模組 130 進行第二次層加密成第二加密電子文檔 160(步驟 330)，完成後再伴隨接收端 20 下載權限清單以及接收端 20 軟體功能關閉權限清單一起傳送至網際網路 50 上之一伺服器 30，傳送端 10 之使用者可於伺服

器 30 上設定接收端 20 之電腦基本資料、第二加密電子文檔 160 之下載記錄清單顯示、以及檔案內容 110 之相關意見回覆資料，且這些資料及設定只能允許傳送端 10 之使用者可以看見，並依照使用者所設定之接收端 20 下載權限清單(如：收件者名稱、電子郵件位址、及帳號)，於驗證模組 230 設定下載權限後，便將第二加密電子文檔 160 儲存於一資料庫 40(步驟 335)。上述之檔案金鑰 120 及共同金鑰 150 係為一組預定長度之數位位元，在本發明之最佳實施例之長度是採用 256bits，以增加安全性。

而接收端 20 進行下載傳送端 10 所傳來之資料時，請參照「第 1b 圖」，此為接收端 20 下載並解密檔案內容 110 之系統架構示意圖，請一併參照「第 2b 圖」，此為接收端 20 下載並解密檔案內容 110 之方法流程圖。當接收端 20 之使用者收到電子郵件 220 通知有檔案內容 110 需下載時，可對電子郵件 220 所夾帶之檔案內容摘要 170 及檔案金鑰 120 以共同金鑰 150 進行下載(步驟 340)，並進行確認電子郵件 220 所夾帶檔案確實為接收端 20 之共同金鑰 150 可解密(步驟 345)。

若確認無誤，則使用者即可自解密模組 210 以共同金鑰 150 進行解密，而可得到檔案內容摘要 170 中之主旨、摘要及部分內容(步驟 350)，以及包含一組可進入伺服器 30 之權限，例如一組透過加入權限設定之 link 網址，或者在驗證模組 230 及設定可下載權限之接收端 20 使用者之登入帳號或是電子郵

件位址，接收端 20 使用者便可以自己的帳號進行登入，或是透過該 link 網址來進行登入，伺服器 30 之驗證模組 230 便可確認登入之使用者是否符合權限設定(步驟 355)，驗證模組 230 比對傳送端 10 使用者所設定之身分認證無誤後，便可下載伺服器 30 之資料庫 40 中內容摘要所對應之第二加密電子文檔 160 (步驟 360)。

下載完成後，可於驗證模組 230 中記錄下載者登入之時間、帳號、網路位址(IP address)、網路卡序號(MAC address)等接收端電腦資料。然後，同樣先由解密模組 210 以共同金鑰 150 進行解密對下載之第二加密電子文檔 160 進行第一次解密，而可獲得第一加密電子文檔 140(步驟 365)；接著，編輯程式 100 便可以先前所接收之檔案金鑰 150 對第一加密電子文檔 140 再進行第二層解密，依據接收端 20 軟體功能關閉權限清單還原成功能受限之檔案內容 110(例如：滑鼠右鍵功能鎖定、禁止修改、複製、列印或存檔…等功能)，接收端 20 並可在閱讀完後在伺服器 30 上留下相關意見回覆資料，而傳送端 10 可連線至伺服器 30 進行查詢，便可得知有哪些信件中之收件者已經下載了傳送之檔案內容 110，以及對該檔案內容 110 之意見進行瀏覽。

透過本發明所揭露之方法，不僅可利用共同金鑰 150 達成第一層安全防護，使用者即便是進行單純的檔案讀取，在存檔時即已進行了第一次加密，而可以使得不具相同之共同金鑰

150 之編輯程式 100 無法開啟；而在本發明所揭露之架構下進行傳送時，接收端 20 只會接收到以共同金鑰 150 加密過之檔案內容摘要 170 以及檔案金鑰 120，則可避免接收端 20 直接獲得加密之檔案內容 110 本身，而增加了被破解密碼之機會，而且藉由伺服器 30 之中央控管方式，傳送端 10 可以很清楚的掌控哪些接收端 20 已經進行下載資料之動作，對伺服器 30 而言，由於接收端 20 所進行下載之時間可能皆不相同，而較傳送端 10 同時間直接傳檔案內容 110 給多個接收端 20，更可減低該時間點上網路之流量負擔。

雖然本發明以前述之較佳實施例揭露如上，然其並非用以限定本發明，任何熟習相像技藝者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，因此本發明之專利保護範圍須視本說明書所附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1a 圖、第 1b 圖係本發明之系統架構圖；及

第 2a 圖、第 2b 圖係本發明之方法流程圖。

【主要元件符號說明】

10　傳送端

20　接收端

30　伺服器

40　資料庫

50　網際網路

100	編輯程式
110	檔案內容
120	檔案金鑰
130	加密模組
140	第一加密電子文檔
150	共同金鑰
160	第二加密電子文檔
170	檔案內容摘要
210	解密模組
220	電子郵件
230	驗證模組

五、中文發明摘要：

一種保護數位資料之系統及其方法，當傳送端傳送檔案內容至接收端時，編輯程式先以檔案金鑰編成第一加密電子文檔及擷取出檔案內容摘要，再以共同金鑰將第一加密電子文檔編成第二加密電子文檔存於伺服器之資料庫，而檔案金鑰及檔案內容摘要也以共同金鑰加密後傳至接收端；當接收端以共同金鑰進行解密取得檔案內容摘要，及進入伺服器之允許權限時，即可進行下載第二加密電子文檔後，便可以共同金鑰將第二加密電子文檔解密成第一加密電子文檔；最後，當接收端以編輯程式進行開啟動作時，便以檔案金鑰進行開啟檔案內容，達成保護數位資料功效。

六、英文發明摘要：

十、申請專利範圍：

1. 一種保護數位資料之系統，該系統具有一傳送端、一個以上接收端及一伺服器，其特徵在於該傳送端可傳送一檔案內容至各該接收端時，可達成各該接收端只接收到該傳送端所傳來之以一共同金鑰加密後之一檔案金鑰及一檔案內容摘要，而各該接收端可據此再至該伺服器下載兩層加密後之該檔案內容，而在該傳送端具有：

一編輯程式，用以選取一檔案金鑰對該檔案內容進行第一次加密成一第一加密電子文檔，並擷取該檔案內容摘要；及

一加密模組，用以根據該共同金鑰對該檔案內容進行第二層加密而產生一第二加密電子文檔，以及對該檔案金鑰及該檔案內容摘要於傳送時以該共同金鑰進行加密。

2. 如申請專利範圍第 1 項所述之系統，其中該伺服器還具有一驗證模組，用以記錄該傳送端設定之該第二加密電子文檔可進行下載之各該接收端之權限。

3. 如申請專利範圍第 2 項所述之系統，其中該驗證模組可於各該接收端下載完成後記錄各接收端之一登入時間，一登入帳號，一網路位址(IP address)，及一網路卡序號(MAC address)。

4. 如申請專利範圍第 1 項所述之系統，其中該第二加密電子文檔係儲存於與該伺服器連線之一資料庫中。

5. 如申請專利範圍第 1 項所述之系統，其中該接收端包含：

一解密模組，用以該共同金鑰對該第二加密電子文檔進

行解密成該第一加密電子文檔；及

一編輯程式，用以根據該檔案金鑰對該第一加密電子文檔進行解密成該檔案內容。

6. 如申請專利範圍第 5 項所述之系統，其中該編輯程式可依據一接收端軟體功能關閉權限清單進行該檔案內容之功能限定。

7. 如申請專利範圍第 1 項所述之系統，其中該檔案金鑰及該檔案內容摘要係以一電子郵件之方式進行傳遞。

8. 如申請專利範圍第 1 項所述之系統，其中該傳送端係可至該伺服器查詢各該接收端之下載記錄。

9. 一種保護數位資料之方法，該方法在一傳送端進行傳送一檔案內容時，包含下列步驟：

以一檔案金鑰將該檔案內容加密成一第一加密電子文檔；

傳送時，擷取出該檔案內容之一檔案內容摘要；

以一共同金鑰對該第一加密電子文檔加密成一第二加密電子文檔；

傳送該第二加密電子文檔至一伺服器；及

傳送該檔案金鑰及該檔案內容摘要至一個以上之接收端。

10. 如申請專利範圍第 9 項所述之方法，其中該方法在該接收端進行接收該檔案內容時，包含下列步驟：

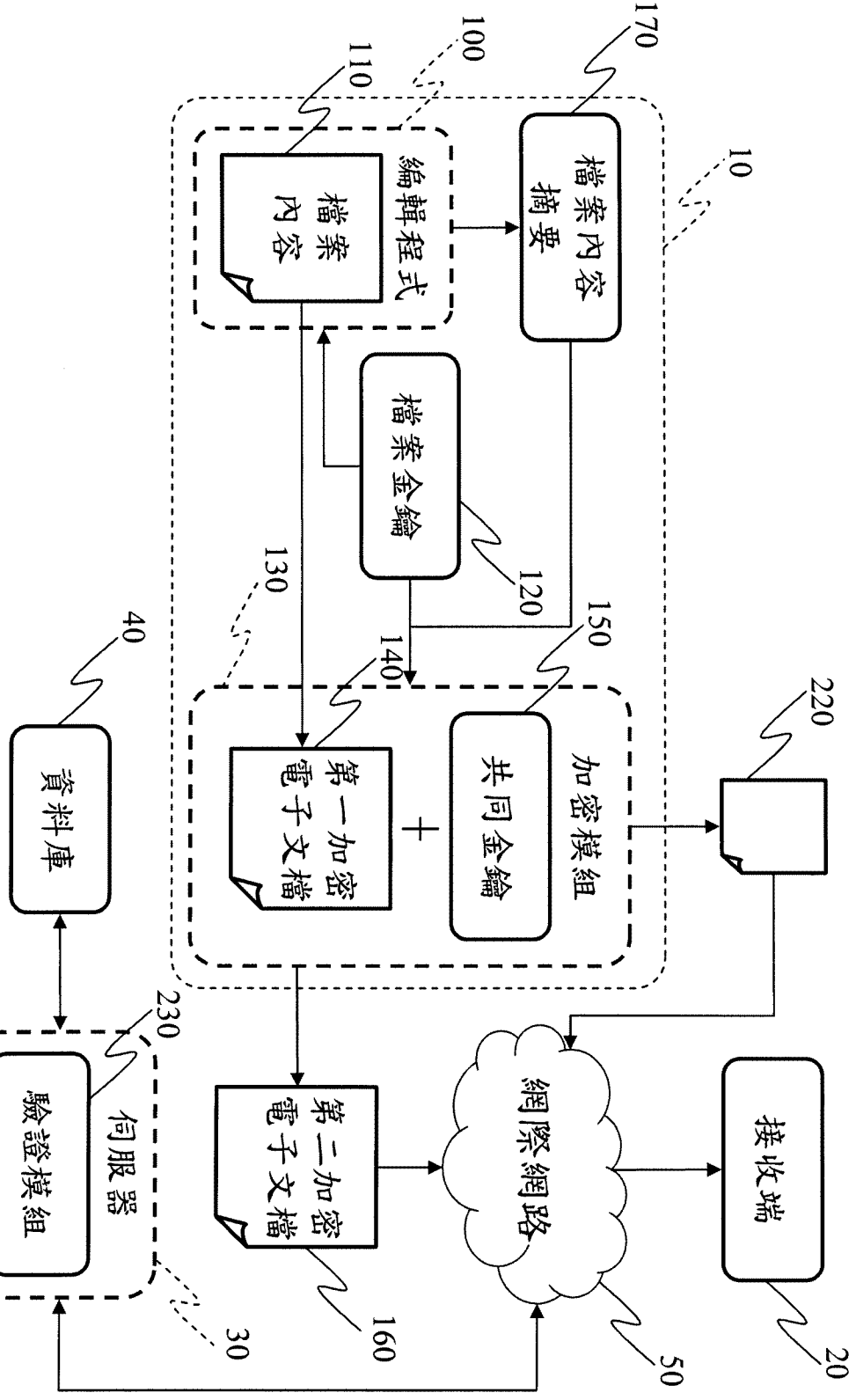
接收該傳送端傳來之該檔案金鑰及該檔案內容摘要；

登入該伺服器下載該檔案內容摘要對應之該第二加密電子文檔；

以該共同金鑰對該第二加密電子文檔解密成該第一加密電子文檔；及

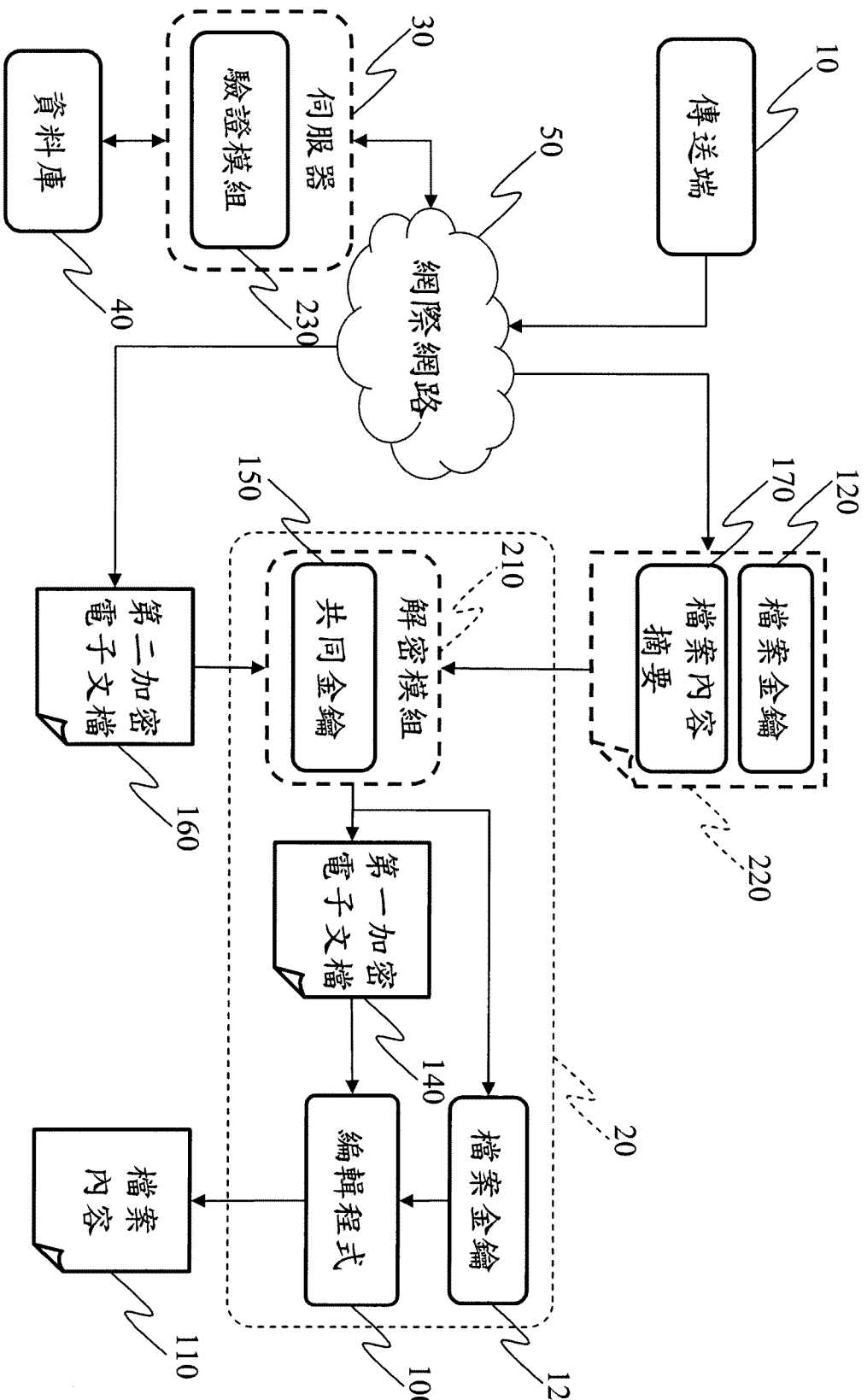
以該檔案金鑰進行該第一加密電子文檔解密成該檔案內容。

圖式


檔案內容摘要
編輯程式
檔案內容
檔案金鑰
加密模組
共同金鑰
+
第一加密電子文檔
資料庫
伺服器
驗證模組
第二加密電子文檔
網際網路
接收端
10
20
30
40
50
100
110
120
130
140
150
160
170
220
230

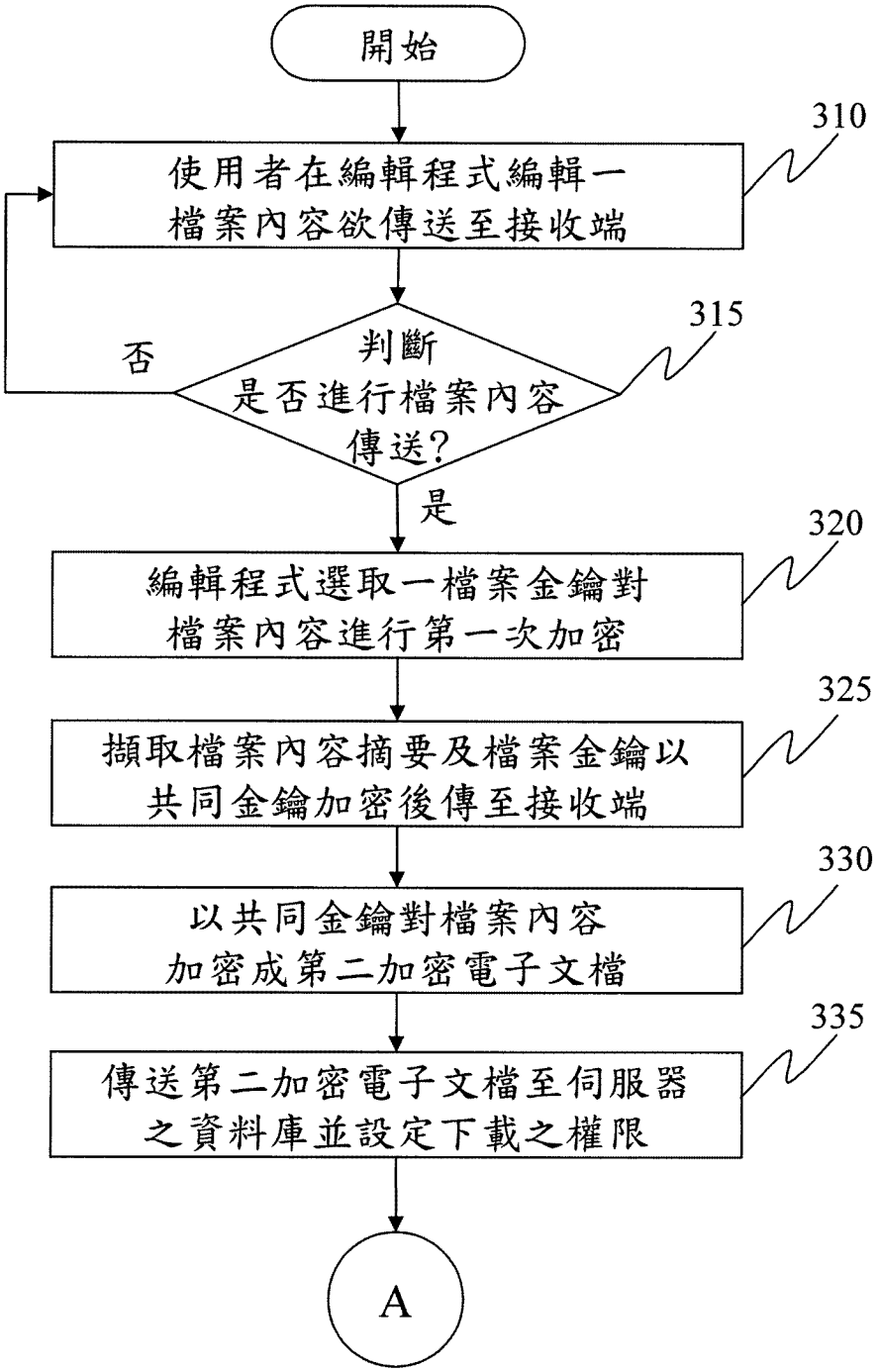
第 1a 圖

圖式


傳送端
10
伺服器
30
驗證模組
資料庫
40
網際網路
50
230
檔案金鑰
檔案內容摘要
120
170
220
解密模組
210
150
共同金鑰
第二加密電子文檔
160
第一加密電子文檔
140
檔案金鑰
編輯程式
檔案內容
110
100
120
20

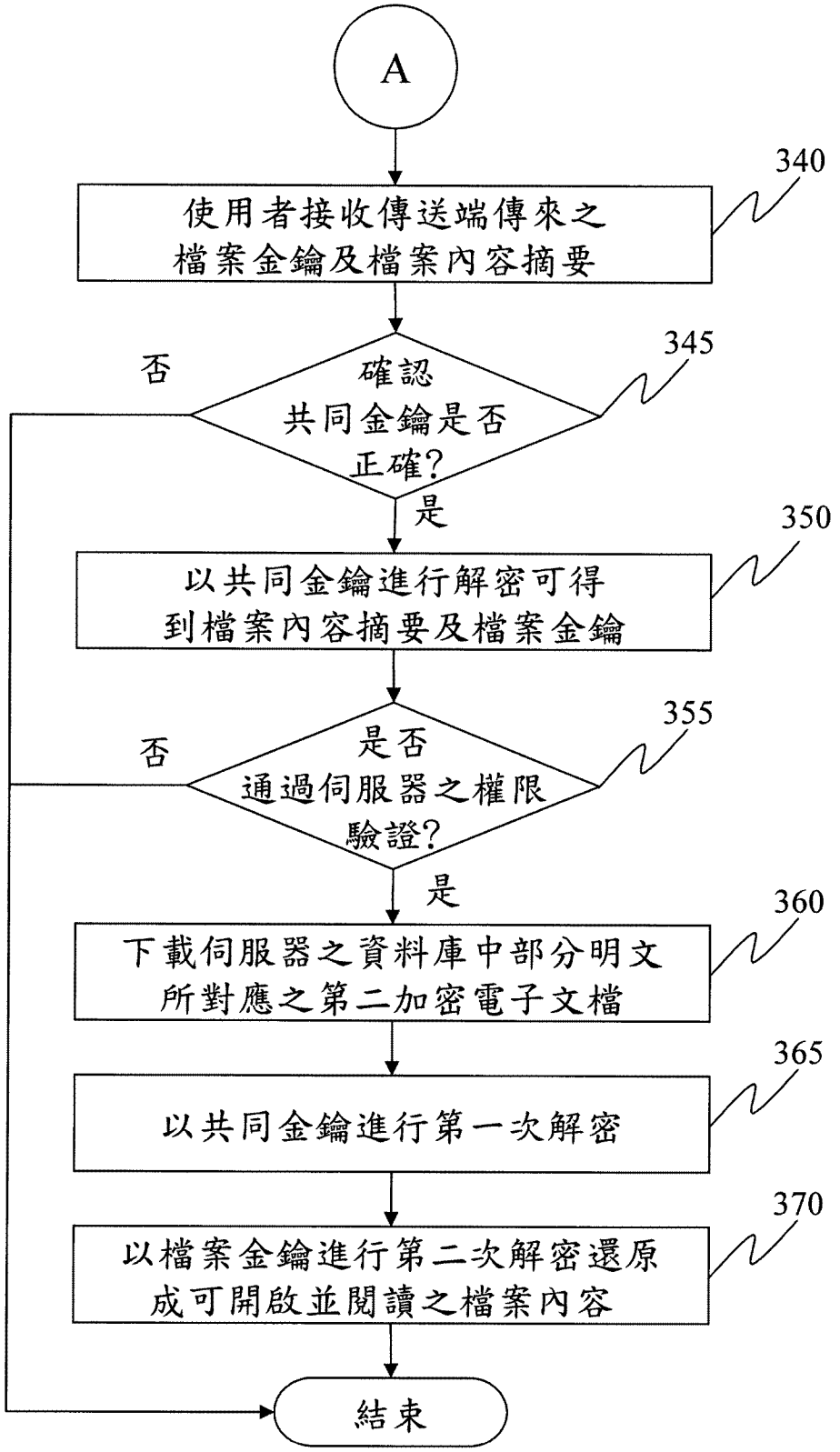
第 1b 圖

圖式


開始
310
使用者在編輯程式編輯一
檔案內容欲傳送至接收端
315
判斷
是否進行檔案內容
傳送?
否
是
320
編輯程式選取一檔案金鑰對
檔案內容進行第一次加密
325
擷取檔案內容摘要及檔案金鑰以
共同金鑰加密後傳至接收端
330
以共同金鑰對檔案內容
加密成第二加密電子文檔
335
傳送第二加密電子文檔至伺服器
之資料庫並設定下載之權限
A

第 2a 圖

圖式


A
340
使用者接收傳送端傳來之
檔案金鑰及檔案內容摘要
345
確認
共同金鑰是否
正確?
否
是
350
以共同金鑰進行解密可得
到檔案內容摘要及檔案金鑰
355
是否
通過伺服器之權限
驗證?
否
是
360
下載伺服器之資料庫中部分明文
所對應之第二加密電子文檔
365
以共同金鑰進行第一次解密
370
以檔案金鑰進行第二次解密還原
成可開啟並閱讀之檔案內容
結束

第 2b 圖

七、指定代表圖：

(一)本案指定代表圖為：第（ 1a、1b ）圖。

(二)本代表圖之元件符號簡單說明:

10	傳送端
20	接收端
30	伺服器
40	資料庫
50	網際網路
100	編輯程式
110	檔案內容
120	檔案金鑰
130	加密模組
140	第一加密電子文檔
150	共同金鑰
160	第二加密電子文檔
170	檔案內容摘要
210	解密模組
220	電子郵件
230	驗證模組

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。