(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201310959 A1
(43)公開日： 中華民國 102 (2013) 年 03 月 01 日

(21)申請案號：100131432 (22)申請日： 中華民國 100 (2011) 年 08 月 31 日
(51)Int. Cl.： *H04L9/32 (2006.01)* *H04L9/28 (2006.01)*
H04L12/26 (2006.01)
(71)申請人：萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國
(72)發明人：趙志文 CHAO, WINSON (TW) ；孫維孝 SUEN, WILL WS (TW) ；吳明勳 WU, TRAVIS MH (TW) ；余盈鋐 YU, YING HUNG (TW) ；林大維 LIN, DAVE TW (TW)
(74)代理人：蔡玉玲
申請實體審查：有 申請專利範圍項數：7 項 圖式數：7 共 34 頁

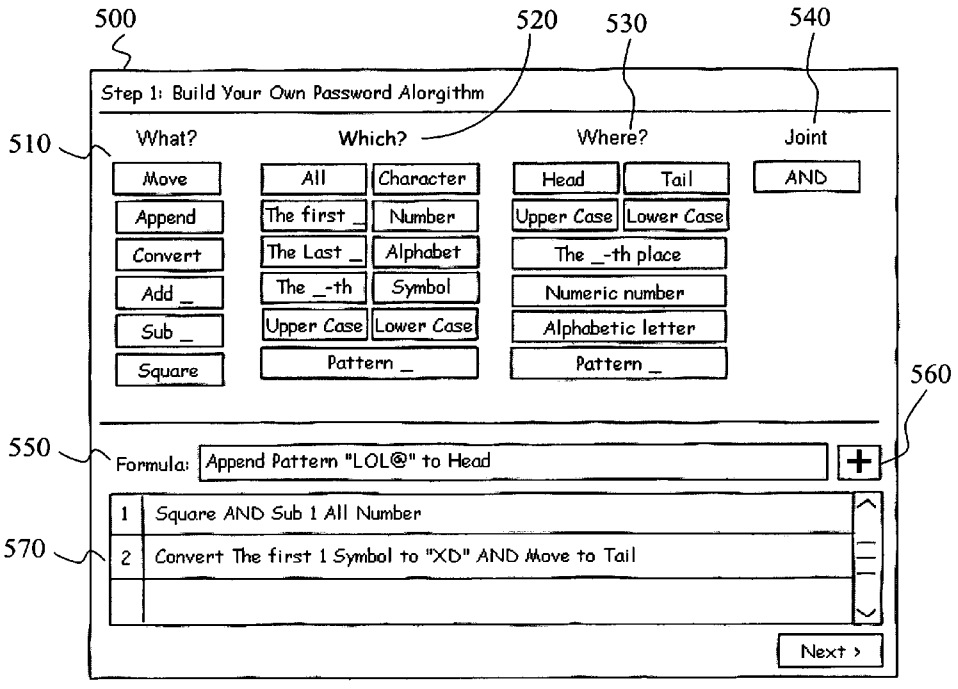
(54)名稱

動態提供演算式密碼／盤問鑑定的方法與電腦裝置

METHOD AND COMPUTER SYSTEM FOR DYNAMICALLY PROVIDING ALGORITHM-BASED PASSWORD/CHALLENGE AUTHENTICATION

(57)摘要

本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含：(a)回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及(c)回應來自該用戶端電腦該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。



201310959

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：100131432 H04L 9/32 (2006.01)

※ 申請日：100 年 08 月 31 日 ※IPC 分類：H04L 9/38 (2006.01)

H04L 12/56 (2006.01)

一、發明名稱：（中文/英文）

動態提供演算式密碼/盤問鑑定的方法與電腦裝置

METHOD AND COMPUTER SYSTEM FOR DYNAMICALLY PROVIDING ALGORITHM-BASED PASSWORD/CHALLENGE AUTHENTICATION

二、中文發明摘要：

本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

三、英文發明摘要：

Disclosed are a method for dynamically providing algorithm-based password/challenge authentication and a computer device using the method. The method comprises the following steps:

(a) in response to a login request to access a web service from a client computer, sending a login webpage, the webpage at least comprising a field of displaying a seed and a field for inputting username; (b) in response to a username from the client computer, sending a seed generated randomly which is displayed in the field of displaying a seed; and (c) in response to the username and a first string as a password converted from the seed based on an algorithm from the client computer, the server comparing the first string and a second string converted from the seed based on an algorithm stored in the server in advance and in associated with the username.

四、指定代表圖：

(一)本案指定代表圖為：圖 5。

(二)本代表圖之元件符號簡單說明：無。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無。

5

六、發明說明：

【發明所屬之技術領域】

本發明係關於提供密碼式盤問鑑定的機制；尤其是動態提供演算式密碼/盤問鑑定的方法與電腦裝置方法與電腦裝置。

【先前技術】

日常生活中使用到各式各樣的資訊裝置，例如行動電話、個人電腦、筆記型電腦、平板電腦等，其中皆可能儲存有使用者的個人資料及身分資料。隨著網路的普及，越來越多的網路應用係以線上作業（on-line）執行。特別是，伺服器為了提供網路服務，例如社交網路服務、網頁郵件服務、行動商務服務、銀行線上交易服務、資料庫存取服務或是內容資訊提供服務等等，也儲存有使用者的個人資料及身分資料，因此為了安全性以及隱私的考量，伺服器一般會要求使用者在使用其服務前，需遵守一鑑定（authentication）程序以確認使用者身份。目前，最常用的是密碼式盤問（password-based challenge）鑑定程序。即伺服器一般會要求使用者在使用其服務前，需先輸入使用者帳號與密碼來進行身份識別(或稱為「登入（login）」)，避免使用者的個人資料被盜取或竄改。

由於網路涵蓋範圍及可及性（accessibility）快速增加，越來越多攻擊目標針對密碼以偽造（fake）使用者的身分。因此，簡單的密碼不再能提供足夠的保護，各種不同機制被提出以提供更佳的保護。例如，要求密碼長度、

複雜性及不可預測性，以獲得抵禦粗暴及字典式搜尋攻擊之密碼強度。此外，要求定期地更改密碼，使舊密碼失效，因而可減少密碼被破解的可能性。這些機制增加安全性，因此能幫助使用者保護其帳號。

然而，如圖 1 所示，客戶端 100 透過網路 140 透過盤問 101 及提供帳號/密碼 102 的鑑定程序，對網站 A 110、網站 B 120、網站 C 130 等要求不同網路服務。實際上多數使用者對不同的網站 A 110、網站 B 120、網站 C 130 等通常使用不同帳號/密碼。這些機制要求使用者必須記住多個存取不同網站之網路服務的密碼。此外，人們往往每天僅登入少數網站，因此通常不易正確無誤地記住那些很少拜訪之網站的密碼。一般情況，使用者必需試著猜密碼，且很可能因太多錯誤嘗試而被鎖住。

因此存在一能幫助使用者記住擾人的密碼且又能維持安全性之需求。習知的動態密碼（one-time password（OTP））技術提供一解決方案。然 OTP 要求額外的技術以提供密碼給使用者。許多情況下，OTP 技術使用一電子裝置。此電子裝置可能遺失，因此增加了遺失密碼的風險。此外，不同組織可能很難分享其 OTP 產生機制。使用者若要存取不同網站提供之網路服務，則將需求不同電子裝置。因此，使用者需隨身攜帶多個電子裝置，這更增加遺失的風險。

一密碼提示（hint）之機制提供了另一解決方案。然，此機制可能降低安全性，因非授權者通常也能看到此密碼

提示，因而能幫助駭客破解密碼。此外，此機制很難對一複雜密碼提供一適當的密碼提示。因此，今日機密的（sensitive）系統很少利用此機制。

習知有許多提供更佳保護之密碼式盤問的方法，例如可參考 WO 2006/020096 A2、WO 2002/017556 A1、美國專利 US 5841871、 US 6094721、美國專利申請公開號 US 2007/0011724 A1 等，在此以引用的方式併入本文。

【發明內容】

本說明書中所提及的特色、優點、或類似表達方式並不暗示本發明可實現的所有特色及優點應在本發明之任何單一的具體實施例內。而是應明白，有關特色及優點的表達方式是指結合具體實施例所述的特定特色、優點、或特性係包含在本發明的至少一具體實施例內。因此，本說明書中對於特色及優點、及類似表達方式的論述可與相同具體實施例有關，但亦非必要。

此外，可以任何合適的方式，在一或多個具體實施例中結合本發明所述特色、優點、及特性。相關技術者應明白，在沒有特定具體實施例之一或多個特定特色或優點的情況下，亦可實施本發明。在其他例子中應明白，特定具體實施例中的其他特色及優點可能未在本發明的所有具體實施例中出現。

本發明提供一新的密碼式盤問機制以識別使用者身

份。該機制提供使用者記住一單一的演算式（algorithm），而不再如習知者去記住多個存取不同網站之網路服務的密碼。該演算式也將被儲存在一要求鑑定之提供網路服務的伺服器中。當使用者登入一網站時，該伺服器將隨機產生一種子（seed）字串（string）（包含字元、符號及數字）提示（prompt）給使用者。使用者再輸入依該使用者記住之演算式將該種子字串轉換為作為密碼之第一串字串。該伺服器再將利用該儲存之演算式轉換該種子字串所得之正確密碼（第二串字串）與使用者輸入的密碼（即第一串字串）作比較。若相同，則登入成功。

根據本發明一實施例，本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生

之一已顯示種子字串及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗；該登入視窗至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該使用者之該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該電腦裝置比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗；該登入視窗至少包含隨機產生之一已顯示種子字串及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該電腦裝置比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

參考以下說明及隨附申請專利範圍或利用如下文所提之本發明的實施方式，即可更加明瞭本發明的這些特色及優點。

【實施方式】

本說明書中「一具體實施例」或類似表達方式的引用是指結合該具體實施例所述的特定特色、結構、或特性係包括在本發明的至少一具體實施例中。因此，在本說明書中，「在一具體實施例中」及類似表達方式之用語的出現未必指相同的具體實施例。

熟此技藝者當知，本發明可實施為電腦裝置、方法或作為電腦程式產品之電腦可讀媒體。因此，本發明可以實施為各種形式，例如完全的硬體實施例、完全的軟體實施例（包含韌體、常駐軟體、微程式碼等），或者亦可實施為軟體與硬體的實施形式，在以下會被稱為「電路」、「模組」或「系統」。此外，本發明亦可以任何有形的媒體形式實施為電腦程式產品，其具有電腦可使用程式碼儲存於其上。

一個或更多個電腦可使用或可讀取媒體的組合都可以利用。舉例來說，電腦可使用或可讀取媒體可以是（但並不限於）電子的、磁的、光學的、電磁的、紅外線的或半導體的系統、裝置、設備或傳播媒體。更具體的電腦可讀取媒體實施例可以包括下列所示（非限定的例示）：由一個或多個連接線所組成的電氣連接、可攜式的電腦磁片、硬碟機、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM 或快閃記憶體)、光纖、可攜式光碟片（CD-ROM）、光學儲存裝置、傳輸媒體（例如網際網路(Internet)或內部網路(intranet)之基礎

連接)、或磁儲存裝置。需注意的是，電腦可使用或可讀取媒體更可以為紙張或任何可用於將程式列印於其上而使得該程式可以再度被電子化之適當媒體，例如籍由光學掃描該紙張或其他媒體，然後再編譯、解譯或其他合適的必要處理方式，然後可再度被儲存於電腦記憶體中。在本文中，電腦可使用或可讀取媒體可以是任何用於保持、儲存、傳送、傳播或傳輸程式碼的媒體，以供與其相連接的指令執行系統、裝置或設備來處理。電腦可使用媒體可包括其中儲存有電腦可使用程式碼的傳播資料訊號，不論是以基頻(baseband)或是部分載波的型態。電腦可使用程式碼之傳輸可以使用任何適體的媒體，包括（但並不限於）無線、有線、光纖纜線、射頻(RF)等。

用於執行本發明操作的電腦程式碼可以使用一種或多種程式語言的組合來撰寫，包括物件導向程式語言（例如 Java、Smalltalk、C++或其他類似者）以及傳統程序程式語言（例如 C 程式語言或其他類似的程式語言）。程式碼可以獨立軟體套件的形式完整的於使用者的電腦上執行或部分於使用者的電腦上執行，或部分於使用者電腦而部分於遠端電腦。

於以下本發明的相關敘述會參照依據本發明具體實施例之電腦裝置、方法及電腦程式產品之流程圖及／或方塊圖來進行說明。當可理解每一個流程圖及／或方塊圖中的每一個方塊，以及流程圖及／或方塊圖中方塊的任何組合，可以使用電腦程式指令來實施。這些電腦程式指令可供通用型電腦或特殊電腦的處理器或其他可程式化資料處理裝置所組成的機器來執行，而指令經由電腦或其他可程式化資料處理裝置處理以便實施流程圖及／或方塊圖中所說明之功能或操作。

這些電腦程式指令亦可被儲存在電腦可讀取媒體上，以便指示電腦或其他可程式化資料處理裝置來進行特定的功能，而這些儲存在電腦可讀取媒體上的指令構成一製成品，其內包括之指令可實施流程圖及／或方塊圖中所說明之功能或操作。

電腦程式指令亦可被載入到電腦上或其他可程式化資料處理裝置，以便於電腦或其他可程式化裝置上進行一系統操作步驟，而於該電腦或其他可程式化裝置上執行該指令時產生電腦實施程序以達成流程圖及／或方塊圖中所說明之功能或操作。

其次，請參照圖 2 至圖 7B，在圖式中顯示依據本發明各種實施例的電腦裝置、方法及電腦程式產品可實施的架構、功能及操作之流程圖及方塊圖。因此，流程圖或方塊圖中的每個方塊可表示一模組、區段、或部分的程式碼，其包含一個或多個可執行指令，以實施指定的邏輯功能。另當注意者，某些其他的實施例中，方塊所述的功能可以不依圖中所示之順序進行。舉例來說，兩個圖示相連接的方塊事實上亦可以同時執行，或依所牽涉到的功能在某些情況下亦可以依圖示相反的順序執行。此外亦需注意者，每個方塊圖及／或流程圖的方塊，以及方塊圖及／或流程圖中方塊之組合，可藉由基於特殊目的硬體的系統來實施，或者藉由特殊目的硬體與電腦指令的組合，來執行特定的功能或操作。

<電腦裝置>

圖 2 說明本發明之例示性服務提供者伺服器 202 之硬體環境方塊圖。在一個示範性的實施例中，伺服器為一台

通用型之桌上型電腦，可具有處理器以執行各種應用程式；儲存裝置以儲存各種資訊及程式碼；顯示裝置、通訊及輸出/入裝置做為與使用者溝通之介面；以及週邊元件或其他特定用途元件。在其他實施例中，本發明亦可實施為其他的形式，而具有更多或更少之其他裝置或元件。網路亦可實施為任何型式之連線，包括固定連接之區域網路(LAN)或廣域網路(WAN)連線，或利用網際網路服務提供者來暫時撥接至網際網路，亦不限於有線無線等各種連接方式，例如透過GSM、或 Wi-Fi 等無線網路與用戶端電腦通信。然而應了解，雖未繪示但其他硬體及軟體組件(例如額外電腦系統、路由器、防火牆等)可包含於網路之中。

如圖 2 所示，伺服器 202 包括一耦合至系統匯流排 206 之處理器單元 204。一視訊配接器 208(其控制一顯示器 210)亦耦合至系統匯流排 206。系統匯流排 206 藉由一匯流排橋 212 耦合至一輸入/輸出(I/O)匯流排 214。一 I/O 介面 216 耦合至 I/O 匯流排 214。I/O 介面 216 能與各個 I/O 裝置之通信，該等 I/O 裝置包括一鍵盤 218、一滑鼠 220、一唯讀光碟機(CD-ROM)222、一軟碟機 224 及一快閃記憶體隨身碟 226。I/O 裝置更可為數位相機模組用以輸入影像資料或是條碼資料，或是 I/O 裝置可與顯示器 210 整合為觸控螢幕，用以供使用者操作應用程式與編寫資訊。連接到 I/O 介面 216 之埠的規格，可以是熟悉電腦架構技術者所知之任一種，其包括(但不限於)通用串列匯流排(USB)埠。

使用一網路介面 230，伺服器 202 能藉由一網路 228 與一用戶端電腦 252 通信，網路介面 230 耦合至系統匯流

排 206。網路 228 可係一外部網路(例如，網際網路)或一內部網路(例如，一乙太網路或一虛擬私人網路(VPN))。使用網路 228，伺服器 202 能使用本發明以與用戶端電腦 252 互動。

一硬碟機介面 232 亦耦合至系統匯流排 206 上。硬碟機介面 232 與一硬碟機 234 介接。在一較佳實施例中，硬碟機 234 進駐（populates）系統記憶體 236，該系統記憶體 236 亦耦合至系統匯流排 206。進駐系統記憶體 236 之資料包括伺服器 202 之作業系統(OS)238 及應用程式 244。

OS 238 包括一用於供使用者存取諸如應用程式 244 等資源之殼層(shell)240 及核心 242。殼層 240 係一可在使用者與作業系統間提供一解譯器與介面的程式。該殼層提供系統提示、解譯由鍵盤、滑鼠或其他使用者輸入媒體所輸入的命令及向該作業系統之適當的較低層級(例如，核心 242)發送經解譯之命令供進行處理。雖然殼層 240 一般係以文字為基礎之行導向式使用者介面，但本發明亦能支援其他使用者介面模式，諸如圖形的、語音的、示意動作的模式等。核心 242 包括 OS 238 之較低層級功能，該等較低層級功能包括由 OS 238 之其他部分及應用程式 244 所要求之基本服務，該基本服務包括：記憶體管理、處理序及任務管理、磁碟管理及滑鼠與鍵盤之管理。

用戶端電腦 252 可以使用與前述伺服器 202 相同或類似的硬體架構，亦或者可以利用其他的基礎架構，本發明並不限制。舉例來說，用戶端電腦可以是桌上型電腦、筆

記型電腦、個人數位助理(PDA)、智慧型手機等。然而圖2所示以及上述的範例皆非用於限制本發明的架構。用戶端電腦 252 可包括一瀏覽器。瀏覽器包括程式模組及指令，該等程式模組及指令使用超文字傳送協定(HTTP)訊息使全球資訊網(WWW)用戶端(即：用戶端電腦252)能夠發送及接收網路訊息至網際網路，因此實現與伺服器 202 通信。

應用程式 244 可包括一本發明之密碼式盤問模組246。密碼式盤問模組 246 包括程式模組及指令，該等程式模組及指令能與用戶端電腦252通信，以確認使用者身份。該密碼式盤問模組246可以是應用程式內之模組，或以常駐程式(Daemon)之方式實施。但在其他實施例中，亦可以用其他形式之程式型態來實施。 該密碼式盤問模組246包括用於實施下文所說明之圖4A及4B內所說明之程序之代碼。

在伺服器 202 內繪示之硬體元件並非意欲包羅萬象，而係代表本發明所使用之最重要元件。舉例而言，伺服器 202 可以另包括替代記憶體儲存裝置，諸如磁帶(magnetic cassette)、多樣化數位光碟(DVD)、(Bernoulli)卡匣及類似者。此等及其它變化將包含在本發明之精神及範疇內

<密碼/盤問鑑定流程>

圖 4A 與圖 4B 係配合圖 3 以顯示伺服器 202 端密碼式盤問模組的方法步驟。圖 5 與圖 6 係配合圖 4A 以顯示

伺服器提示之登錄與確認（verification）之執行畫面。

圖 4A 為一種依據本發明一具體實施例之密碼/盤問鑑定之登錄（registration）的方法流程圖。

- 步驟 400: 伺服器 202 端接收一來自用戶端電腦 252 存取一網務服務之請求。
- 步驟 402: 回應該請求，伺服器 202 送出一登錄網頁 500（如圖 5 所示）。該用戶端電腦 252 之使用者輸入帳號且在該登錄網頁 500 上建立其想要的演算式。
- 步驟 404:回應該用戶端電腦 252 使用者之完成輸入演算式，伺服器 202 端送出一確認網頁 600（如圖 6 所示）並隨機產生一種子字串提示給使用者供確認該演算式。使用者再輸入依該使用者記住之演算式將該種子字串轉換為作為密碼之第一串字串。
- 步驟 406: 伺服器 202 再將利用該使用者輸入之該演算式轉換該種子字串所得之第二串字串與使用者輸入之第一串字串作比較。若相同，則確認成功。回應該成功，伺服器 202 儲存該帳號及該演算式。

圖 5 所示之登錄網頁 500 可包含演算式所需之轉換運算子 510，運算元 Which 520、運算元 Where 530 及邏輯運算子 AND 540。轉換運算子 510 可包含 Move、Append 、Convert、Add_、Sub_及 Square 等等，但本發明並不侷限於此。

運算元 Which 520 指示種子字串中哪些字串要被轉換運算子轉換，例如，所有字串(All)、僅有字元（Character）、僅有數字（Number）、僅有字母（Alphabet）、僅有大寫

字母（Upper Case）、僅有小寫字母（Lower Case）、第"_"字串（The "_"th）、最先第"_"符號（The first "_"symbol）、最後第"_"符號（The last "_"symbol）及一組固定字串（或簡稱"字組"）（Pattern_）等等，但本發明並不侷限於此。其中"_"代表數字。

運算元 Where 530 指示種子字串中那些要被轉換運算子轉換之字串需被轉換到的位置或方式，例如，所有頭部(Head)、尾部（Tail）、轉換為大寫字母（Upper Case）、轉換為小寫字母（Lower Case）、轉換為數字（Numeric number）、轉換為字母（Alphabet letter）、轉換至第"_"位置（The "_"th place）、及轉換為一"字組"（Pattern_）等等，但本發明並不侷限於此。

依據本發明之具體實施例，使用者輸入帳號的網頁（未顯示）與要建立其想要演算式之登錄網頁是不同網頁。但本發明並不侷限於此，在其他不同實施例，輸入帳號的網頁與登錄網頁可以是相同網頁。

如前述，該用戶端電腦 252 之使用者輸入帳號且在該登錄網頁 500 上使用前述轉換運算子 510，運算元 Which 520、運算元 Where 530 及邏輯運算子 AND 540，建立其想要的演算式公式 550。此外，藉由增加符 560，使用者可建立包含一組公式之演算式。當使用者完成其想要的演算式後，可進入一確認網頁 600 進行該演算式之確認。

圖 6 所示之確認網頁 600 可包含一組使用者建立之公

式的演算式 610 及一確認區 620 等等，但本發明並不侷限於此。該確認區 620 包含一種子字串區，一密碼輸入區，一伺服器 202 利用該使用者輸入之該演算式轉換該種子字串所得之第二串字串顯示區及一比對結果區。例如，伺服器 202 隨機產生一第一串字串"6kq3U&;1"，經利用該使用者輸入之該演算式 610 轉換後，獲得一第二串字串"LOL@35kq8U;0XD"。即依該演算式 610 第一式，將種子字串中所有數字取平方再減一；第二式將種子字串中第一個符號（此例為"&"）轉換為"XD"並移至種子字串之尾部；最後，第二式將字組"LOL@" 移至種子字串之頭部。

該種子字串區包含 3 個伺服器 202 隨機產生之種子字串供使用者確認該演算式。至於該種子字串區包含之種子字串的數目可為任意，本發明並不欲設限。至於該種子字串只是利用一般隨機產生技術獲得，如：網址 (http://www.random.org/strings/) 所述之 Random String Generator。本發明係提供字串作為種子，因而也適用於使用終端機登入伺服器的環境。本發明也可提供習知 "CAPTCHA" 影像作為種子供使用者利用，至於"CAPTCHA"影像請參見習知"CAPTCHA"影像之相關產生技術，在此不予贅述。

圖 4B 為一種依據本發明一具體實施例之密碼/盤問鑑定之登入（login）的方法流程圖；圖 4B 係配合圖 3 以顯示伺服器 202 端之方法步驟。圖 3 為一種依據本發明一具體實施例之密碼/盤問鑑定之系統示意圖。

- 步驟 410: 伺服器 310 端回應接收一來自用戶端電腦 300

存取一網務服務之登入請求，送出一登入網頁 700（如圖 7A 所示）。該登入網頁 700 包含伺服器 310 隨機產生之種子字串顯示欄 710，帳號輸入欄 720 及密碼輸入欄 730。

- 步驟 412: 伺服器 310 回應使用者輸入之帳號，送出一隨機產生之顯示在該種子字串顯示欄 710 之一種子字串 301。
- 步驟 414: 伺服器 310 回應使用者輸入依該使用者記住之演算式而將該種子字串轉換作為密碼之第一串字串 303(即 f(種子)) 及使用者帳號，伺服器 310 依該儲存之演算式轉換該種子字串所得之正確密碼（第二串字元）（即 F(種子)）與使用者輸入的密碼（即第一串字元，f(種子)）作比較。若相同（即 f(種子)= F(種子)），則登入成功。
- 步驟 416: 若登入失敗，伺服器 310 可再送出一登入網頁 700'（如圖 7B 所示）。重複步驟 412 及步驟 414 之步驟。

需說明的是，依本發明揭示者，使用者與伺服器間共享的是使用者建立之演算式，而非需定期更改之密碼。在網路上傳輸的密碼是依演算式計算而得的結果，其只有一次有效。因此，縱使密碼被暴露，駭客也不能在使用它。因而，本發明不需再定期更改之密碼。此外，使用者可對所有網站使用該演算式，而不再需記住許多用來登入不同網站以存取網路服務的不同密碼。因此，本發明有習知 OTP 的優點，而無其需要一電子裝置之缺點。

此外，本發明也可適用於一般非使用網路之各式各樣的

資訊裝置，例如行動電話、個人電腦、筆記型電腦、平板電腦等，其中因皆儲存有使用者的個人資料及身分資料，因此也可利用本發明之密碼式盤問模組，而提供單機之應用。該密碼式盤問模組246可以是應用程式內之模組，但在其他實施例中，亦可以用其他形式之程式型態來實施，例如整合入作業系統層次供啟動作業系統時盤問使用者。

在不脫離本發明精神或必要特性的情況下，可以其他特定形式來體現本發明。應將所述具體實施例各方面僅視為解說性而非限制性。因此，本發明的範疇如隨附申請專利範圍所示而非如前述說明所示。所有落在申請專利範圍之等效意義及範圍內的變更應視為落在申請專利範圍的範疇內。

【圖式簡單說明】

為了立即瞭解本發明的優點，請參考如附圖所示的特定具體實施例，詳細說明上文簡短敘述的本發明。在瞭解這些圖示僅描繪本發明的典型具體實施例並因此不將其視為限制本發明範疇的情況下，參考附圖以額外的明確性及細節來說明本發明，圖式中：

圖1為一種習知密碼/盤問鑑定之系統示意圖；

圖2為本發明之例示性服務提供者伺服器202之硬體環境方塊圖；

圖3一為種依據本發明一具體實施例之密碼/盤問鑑定之系統示意圖；

圖4A與圖4B分別為一種依據本發明一具體實施例之密碼/盤問鑑定之登錄（registration）與登入（login）的

方法流程圖；

圖 5 顯示本發明實施例中登錄之執行畫面；

圖 6 顯示本發明實施例中確認（verification）之執行畫面；

圖 7A 與圖 7B 顯示本發明實施例中登入之執行畫面。

【主要元件符號說明】

100 客戶端

101 盤問

102 帳號/密碼

110、120、130 網站 A、網站 B、網站 C

140 網路

202 服務提供者伺服器

204 處理器單元

206 系統匯流排

208 視訊配接器

210 顯示器

212 匯流排橋

214 輸入/輸出(I/O)匯流排

216 I/O 介面

218 鍵盤

220 滑鼠

222 唯讀光碟機(CD-ROM)

224 軟碟機

226 快閃記憶體隨身碟

228 網路

230 網路介面

232 硬碟機介面

234 硬碟機

236 系統記憶體

238 作業系統(OS)

240 殼層(shell)

242 核心

244 應用程式

246 密碼式盤問模組

252 用戶端電腦

300 用戶端電腦

301 種子字串

303 第一串字串

310 伺服器

七、申請專利範圍：

1. 一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

2. 一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一已顯示種子字串及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該伺服器比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

3. 一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視

窗；該登入視窗至少包含隨機產生之一種子字串顯示欄及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該使用者之該使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該電腦裝置比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

4. 一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗；該登入視窗至少包含隨機產生之一已顯示種子字串及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號及依一演算式而將該種子字串轉換作為密碼之第一串字串，該電腦裝置比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字元與該第一串字串。

5. 一種動態提供演算式密碼/盤問鑑定的伺服器，包含：

一主機；該主機包含，

一匯流排系統；

一記憶體，連接到該匯流排系統，其中該記憶體包含一組指令；

一連接到該匯流排系統之處理單元，其中該處理單元執行該組指令，以執行如申請專利範圍第 1 至 4 項之任一項所述之方法。

6. 一種儲存在一電腦可用媒體上之電腦程式產品，包含一電腦可讀程式，供於一電腦上執行時，以實施如申請專利範圍第 1 至 4 項之任一項所述之方法，以在一伺服器中動態提供演算式密碼/盤問鑑定。

7. 一種提供一介面供一使用者操作以動態提供演算式密碼/盤問鑑定的伺服器，包含：

一主機；該主機包含，

一匯流排系統；

一記憶體，連接到該匯流排系統，其中該記憶體包含一組指令；

一連接到該匯流排系統之處理單元，其中該處理單元執行該組指令，以執行如申請專利範圍第 1 至 4 項之任一項所述之方法。

八、圖式：

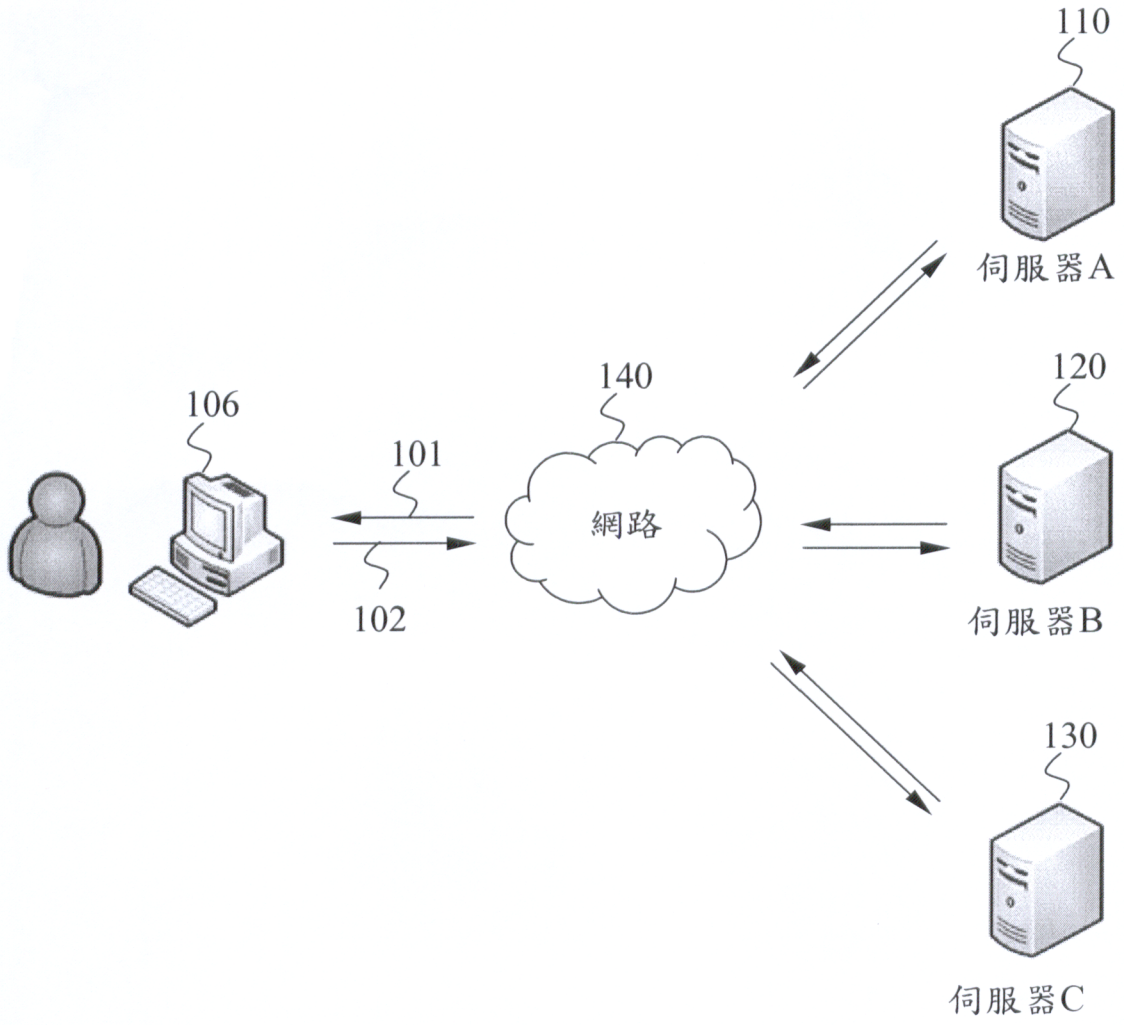


圖1

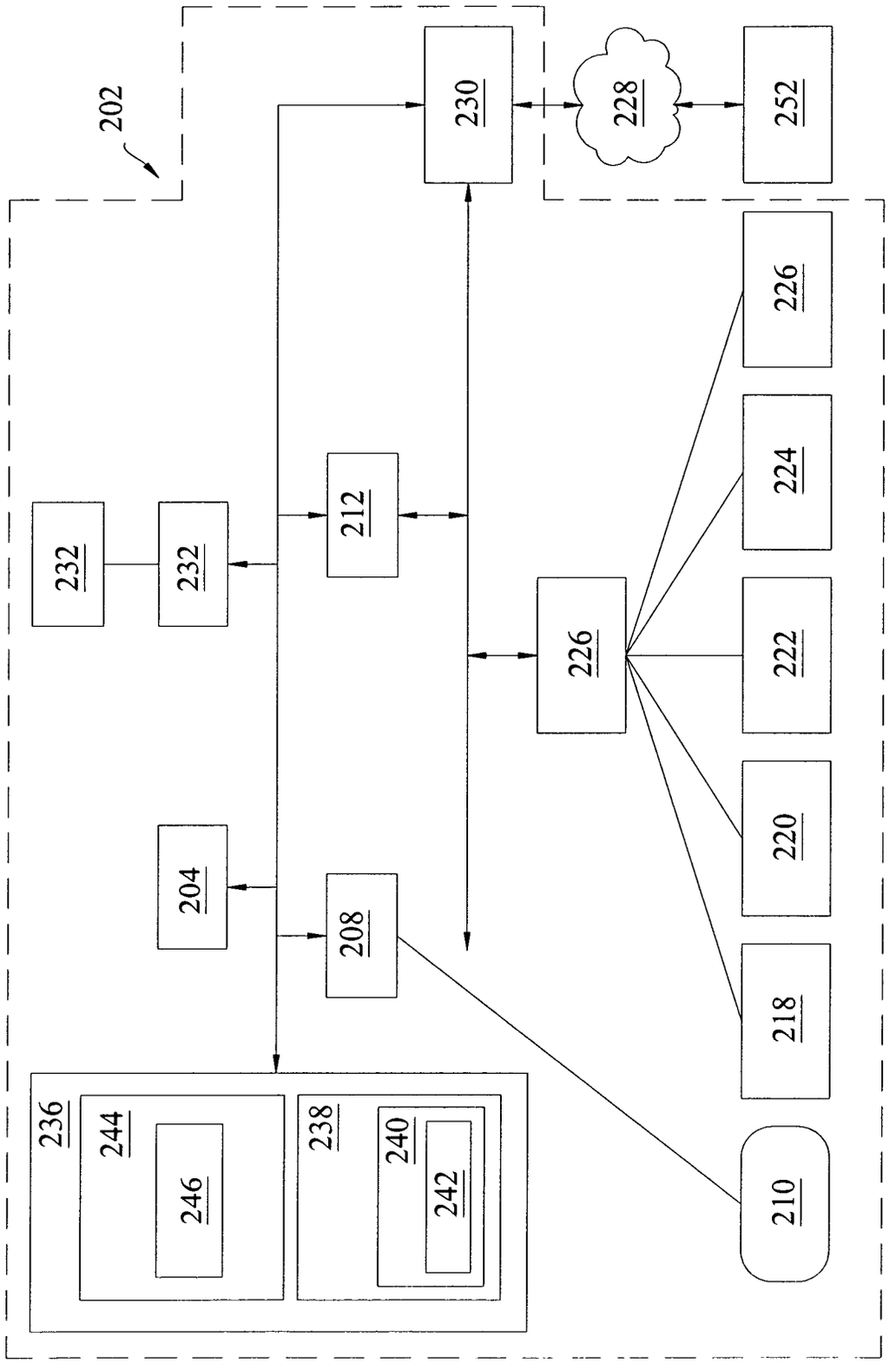

202
230
228
252
226
224
222
220
218
210
212
232
232
226
204
208
236
244
246
238
240
242

圖2

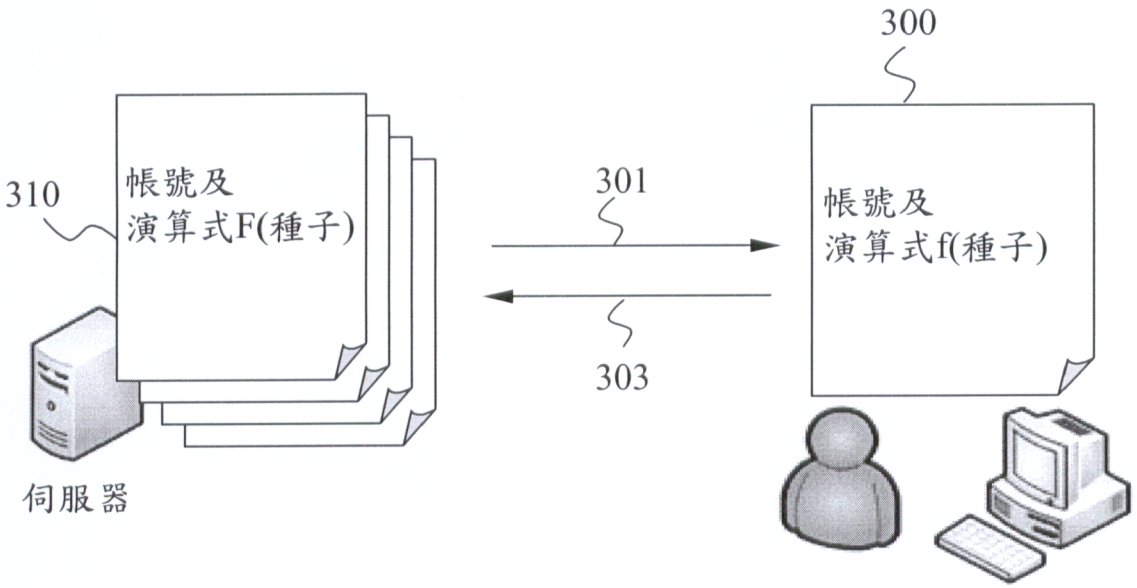


圖3

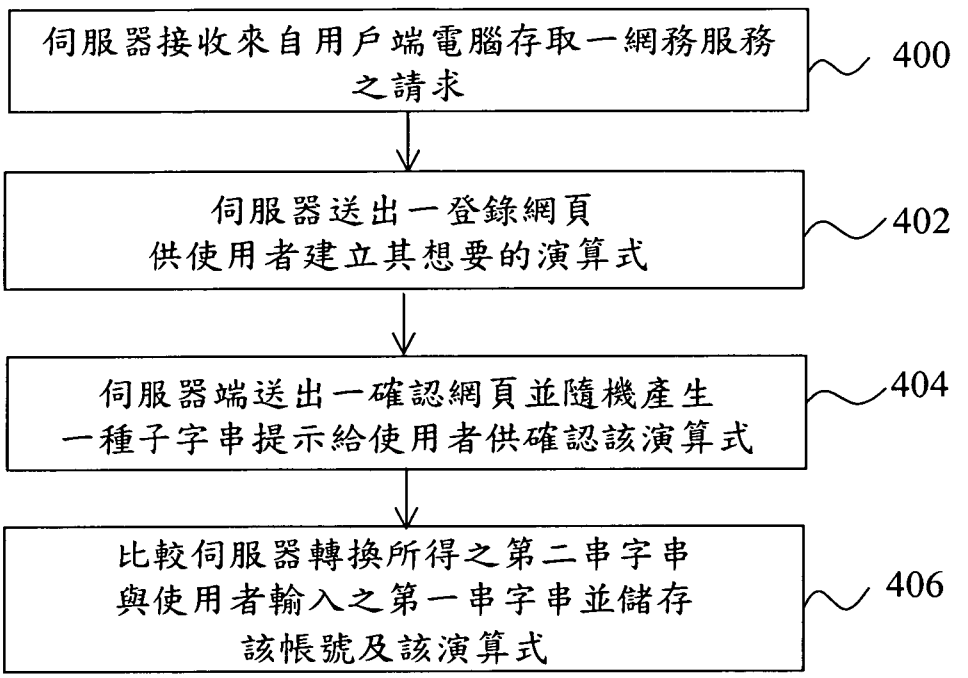

伺服器接收來自用戶端電腦存取一網務服務之請求
400
伺服器送出一登錄網頁供使用者建立其想要的演算式
402
伺服器端送出一確認網頁並隨機產生一種子字串提示給使用者供確認該演算式
404
比較伺服器轉換所得之第二串字串與使用者輸入之第一串字串並儲存該帳號及該演算式
406

圖4A

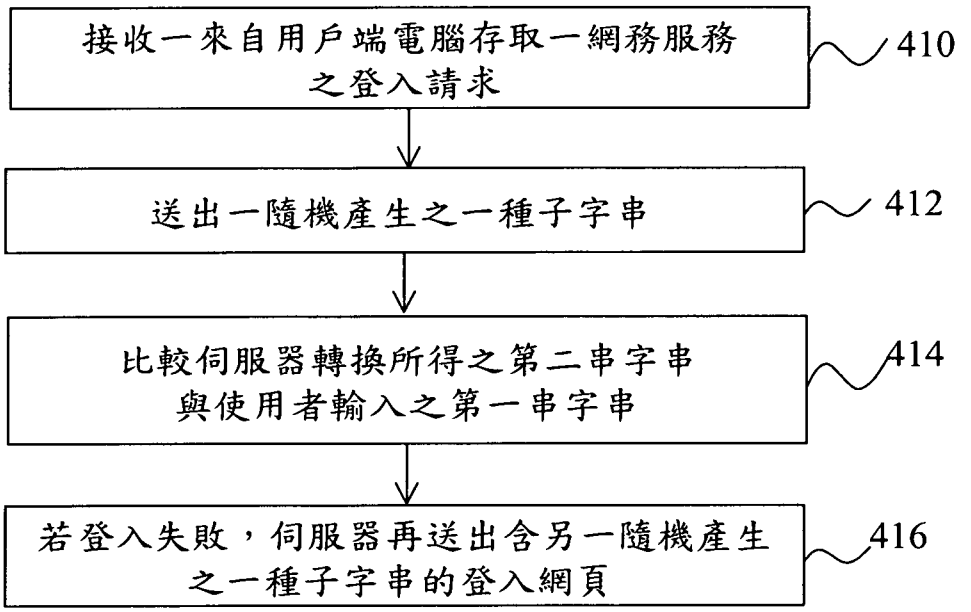

接收一來自用戶端電腦存取一網務服務之登入請求
410
送出一隨機產生之一種子字串
412
比較伺服器轉換所得之第二串字串與使用者輸入之第一串字串
414
若登入失敗，伺服器再送出含另一隨機產生之一種子字串的登入網頁
416

圖4B

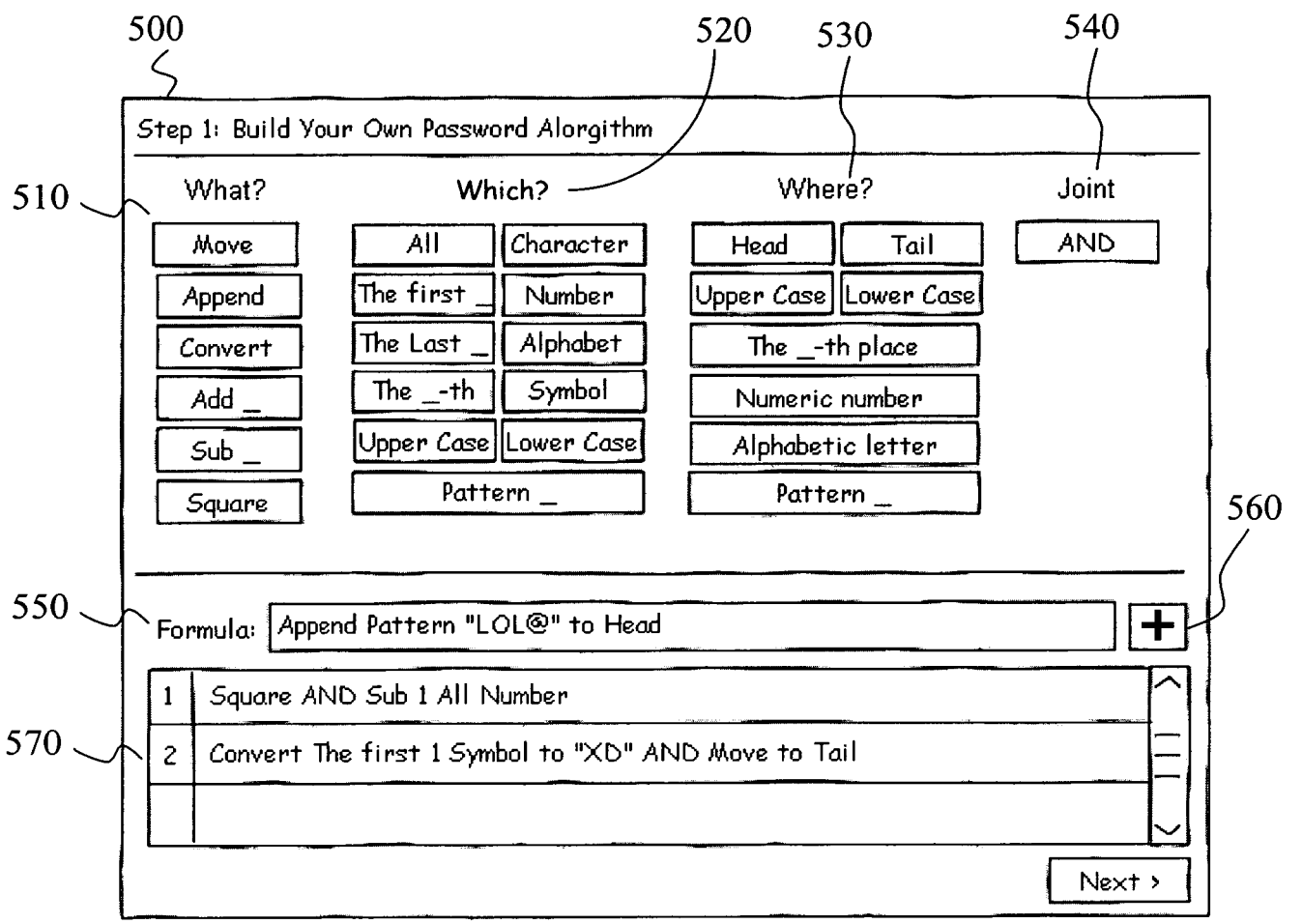

500
520
530
540
Step 1: Build Your Own Password Alorgithm
510
What?
Which?
Where?
Joint
Move
Append
Convert
Add _
Sub _
Square
All
The first _
The Last _
The _-th
Upper Case
Pattern _
Character
Number
Alphabet
Symbol
Lower Case
Head
Tail
Upper Case
Lower Case
The _-th place
Numeric number
Alphabetic letter
Pattern _
AND
560
550
Formula:
Append Pattern "LOL@" to Head
1
Square AND Sub 1 All Number
570
2
Convert The first 1 Symbol to "XD" AND Move to Tail
Next >

圖5

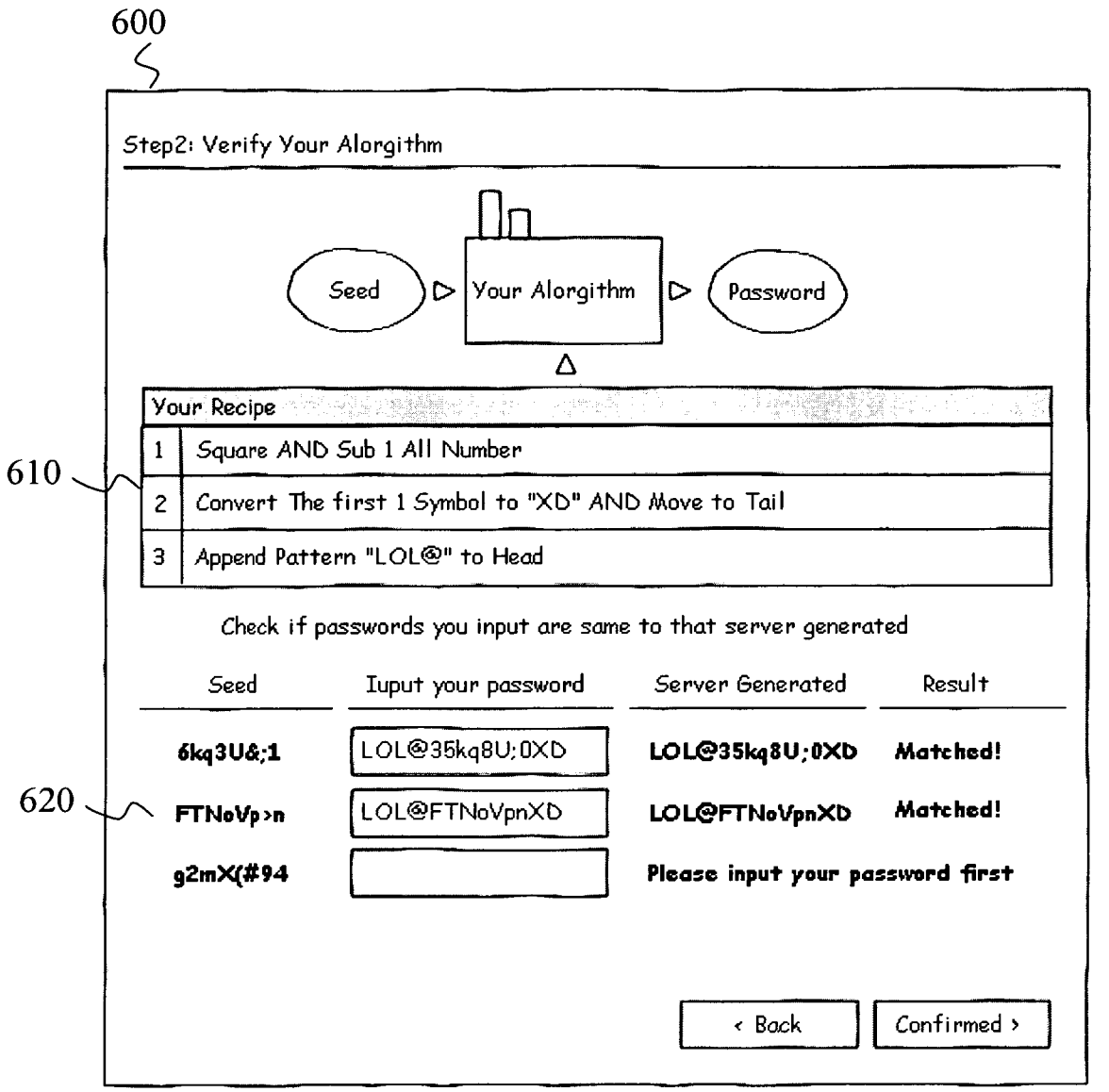

600
Step2: Verify Your Alorgithm
Seed
Your Alorgithm
Password
Your Recipe
1
Square AND Sub 1 All Number
2
Convert The first 1 Symbol to "XD" AND Move to Tail
3
Append Pattern "LOL@" to Head
610
Check if passwords you input are same to that server generated
Seed
Iuput your password
Server Generated
Result
6kq3U&;1
LOL@35kq8U;0XD
LOL@35kq8U;0XD
Matched!
620
FTNoVp>n
LOL@FTNoVpnXD
LOL@FTNoVpnXD
Matched!
g2mX(#94
Please input your password first
< Back
Confirmed >

圖6

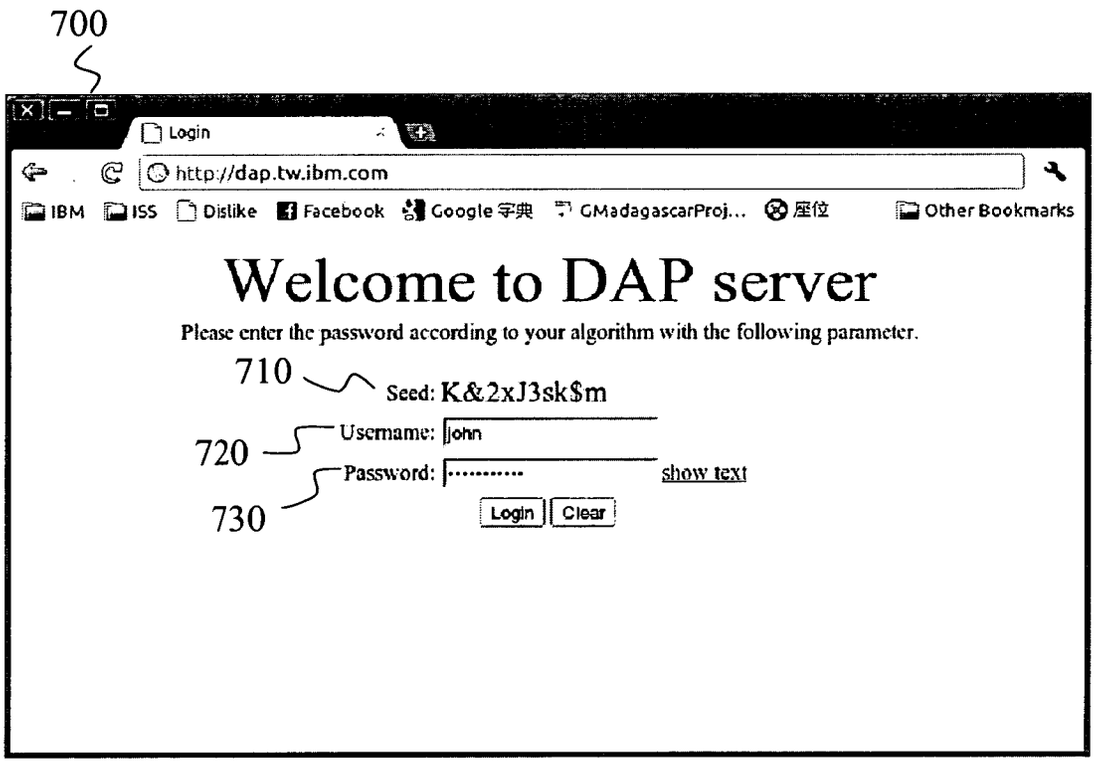

700
Login
http://dap.tw.ibm.com
IBM
ISS
Dislike
Facebook
Google 字典
GMadagascarProj...
座位
Other Bookmarks
Welcome to DAP server
Please enter the password according to your algorithm with the following parameter.
710
Seed: K&2xJ3sk$m
720
Username: john
Password:
show text
730
Login
Clear

圖7A

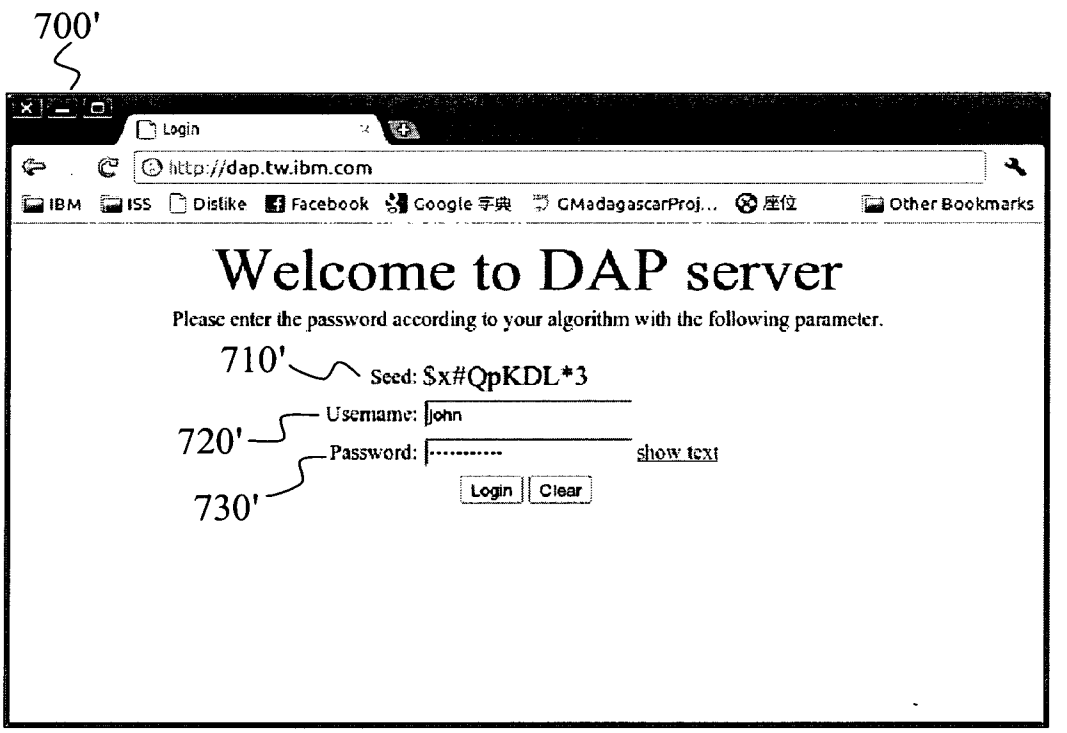

700'
Login
http://dap.tw.ibm.com
IBM
ISS
Dislike
Facebook
Google 字典
GMadagascarProj...
座位
Other Bookmarks
Welcome to DAP server
Please enter the password according to your algorithm with the following parameter.
710'
Seed: $x#QpKDL*3
720'
Username: john
Password:
show text
730'
Login
Clear

圖7B

201310959

案號：100131432
100 年 10 月 07 日修正-替換頁

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：100131432

※ 申請日：100 年 08 月 31 日　　※IPC 分類：H04L 9/32 2006.01
H04L 9/38 2006.01
H04L 12/56 2006.01

一、發明名稱：（中文/英文）

動態提供演算式密碼/盤問鑑定的方法與電腦裝置

METHOD AND COMPUTER SYSTEM FOR DYNAMICALLY PROVIDING ALGORITHM-BASED PASSWORD/CHALLENGE AUTHENTICATION

二、中文發明摘要：

本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

三、英文發明摘要：

Disclosed are a method for dynamically providing algorithm-based password/challenge authentication and a computer

201310959

案號：100131432
100 年 10 月 07 日修正-替換頁

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：100131432

※ 申請日：100 年 08 月 31 日　　※IPC 分類：H04L 9/32 2006.01
H04L 9/38 2006.01
H04L 12/56 2006.01

一、發明名稱：（中文/英文）

動態提供演算式密碼/盤問鑑定的方法與電腦裝置

METHOD AND COMPUTER SYSTEM FOR DYNAMICALLY PROVIDING ALGORITHM-BASED PASSWORD/CHALLENGE AUTHENTICATION

二、中文發明摘要：

本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

三、英文發明摘要：

Disclosed are a method for dynamically providing algorithm-based password/challenge authentication and a computer

device using the method. The method comprises the following steps: (a) in response to a login request to access a web service from a client computer, sending a login webpage, the webpage at least comprising a field of displaying a seed and a field for inputting username; (b) in response to a username from the client computer, sending a seed generated randomly which is displayed in the field of displaying a seed; and (c) in response to the username and a first string as a password converted from the seed based on an algorithm from the client computer, comparing the first string and a second string converted from the seed based on an algorithm stored in the server in advance and in associated with the username.

四、指定代表圖：

(一)本案指定代表圖為：圖 5。

(二)本代表圖之元件符號簡單說明：無。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無。

六、發明說明：

【發明所屬之技術領域】

本發明係關於提供密碼式盤問鑑定的機制；尤其是動態提供演算式密碼/盤問鑑定的方法與電腦裝置方法與電腦裝置。

【先前技術】

日常生活中使用到各式各樣的資訊裝置，例如行動電話、個人電腦、筆記型電腦、平板電腦等，其中皆可能儲存有使用者的個人資料及身分資料。隨著網路的普及，越來越多的網路應用係以線上作業（on-line）執行。特別是，伺服器為了提供網路服務，例如社交網路服務、網頁郵件服務、行動商務服務、銀行線上交易服務、資料庫存取服務或是內容資訊提供服務等等，也儲存有使用者的個人資料及身分資料，因此為了安全性以及隱私的考量，伺服器一般會要求使用者在使用其服務前，需遵守一鑑定（authentication）程序以識別使用者身份。目前，最常用的是密碼式盤問（password-based challenge）鑑定程序。即伺服器一般會要求使用者在使用其服務前，需先輸入使用者帳號與密碼來進行身份識別(或稱為「登入（login）」)，避免使用者的個人資料被盜取或竄改。

由於網路涵蓋範圍及可及性（accessibility）快速增加，越來越多攻擊目標針對密碼以偽造（fake）使用者的身分。因此，簡單的密碼不再能提供足夠的保護，各種不同機制被提出以提供更佳的保護。例如，要求密碼長度、

複雜性及不可預測性，以獲得抵禦粗暴及字典式搜尋攻擊之密碼強度。此外，要求定期地更改密碼，使舊密碼失效，因而可減少密碼被破解的可能性。這些機制增加安全性，因此能幫助使用者保護其帳號。

然而，如圖 1 所示，客戶端 100 透過網路 140 透過盤問 101 及提供帳號/密碼 102 的鑑定程序，對網站 A 110、網站 B 120、網站 C 130 等要求不同網路服務。實際上多數使用者對不同的網站 A 110、網站 B 120、網站 C 130 等通常使用不同帳號/密碼。這些機制要求使用者必須記住多個存取不同網站之網路服務的密碼。此外，人們往往每天僅登入少數網站，因此通常不易正確無誤地記住那些很少拜訪之網站的密碼。一般情況，使用者必需試著猜密碼，且很可能因太多錯誤嘗試而被鎖住。

因此存在一能幫助使用者記住擾人的密碼且又能維持安全性之需求。習知的動態密碼（one-time password（OTP））技術提供一解決方案。然 OTP 要求額外的技術以提供密碼給使用者。許多情況下，OTP 技術使用一電子裝置。此電子裝置可能遺失，因此增加了遺失密碼的風險。此外，不同組織可能很難分享其 OTP 產生機制。使用者若要存取不同網站提供之網路服務，則將需求不同電子裝置。因此，使用者需隨身攜帶多個電子裝置，這更增加遺失的風險。

一密碼提示（hint）之機制提供了另一解決方案。然，

此機制可能降低安全性，因非授權者通常也能看到此密碼提示，因而能幫助駭客破解密碼。此外，此機制很難對一複雜密碼提供一適當的密碼提示。因此，今日機密的（sensitive）系統很少利用此機制。

習知有許多提供更佳保護之密碼式盤問的方法，例如可參考 WO 2006/020096 A2、WO 2002/017556 A1、美國專利 US 5841871、 US 6094721、美國專利申請公開號 US 2007/0011724 A1 等，在此以引用的方式併入本文。

【發明內容】

本說明書中所提及的特色、優點、或類似表達方式並不暗示本發明可實現的所有特色及優點應在本發明之任何單一的具體實施例內。而是應明白，有關特色及優點的表達方式是指結合具體實施例所述的特定特色、優點、或特性係包含在本發明的至少一具體實施例內。因此，本說明書中對於特色及優點、及類似表達方式的論述可與相同具體實施例有關，但亦非必要。

此外，可以任何合適的方式，在一或多個具體實施例中結合本發明所述特色、優點、及特性。相關技術者應明白，在沒有特定具體實施例之一或多個特定特色或優點的情況下，亦可實施本發明。在其他例子中應明白，特定具體實施例中的其他特色及優點可能未在本發明的所有具體實施例中出現。

本發明提供一新的密碼式盤問機制以識別使用者身份。該機制提供使用者記住一單一的演算式（algorithm），而不再如習知者去記住多個存取不同網站之網路服務的密碼。該演算式也將被儲存在一要求鑑定之提供網路服務的伺服器中。當使用者登入一網站時，該伺服器將隨機產生一種子（seed）字串（string）（包含字元、符號及數字）提示（prompt）給使用者。使用者再輸入依該使用者記住之演算式將該種子字串轉換為作為密碼之第一串字串。該伺服器再將利用該儲存之演算式轉換該種子字串所得之正確密碼（第二串字串）與使用者輸入的密碼（即第一串字串）作比較。若相同，則登入成功。

根據本發明一實施例，本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串及一帳號輸入欄；以及

(b)回應來自該用戶端電腦之一使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗;該登入視窗至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該使用者之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

根據本發明另一實施例，本發明揭示一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗；該登入視窗至少包含隨機產生之一種子字串及一帳號輸入欄；以及

(b)回應來自該使用者輸入之一使用者帳號及依一演算

式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

根據本發明又一實施例，本發明揭示一種在一伺服器中登錄一密碼式盤問之演算式的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之請求，送出一登錄網頁，該登錄網頁至少包含建立演算式所需之複數個轉換運算子，複數個運算元及一邏輯運算子；

(b) 回應來自該用戶端電腦之一使用者帳號及一演算式，送出一確認網頁，該確認網頁至少包含隨機產生一種子字串提示給該用戶端電腦供確認該演算式；

(c) 回應來自該用戶端電腦之依該演算式而將該種子字串轉換成作為密碼之第一串字串，該伺服器比較依該演算式轉換該種子字串所得之第二串字串與該第一串字串以確認該演算式；以及

（d）回應該確認，儲存該帳號及該演算式。

最後，根據本發明又一實施例，本發明揭示一種在一電腦裝置中登錄一密碼式盤問之演算式的方法，該方法包含:

(a) 回應接收一來自一使用者存取一網務服務之請求，送出一登錄視窗，該登錄視窗至少包含建立演算式所需之複數個轉換運算子，複數個運算元及一邏輯運算子；

(b) 回應來自該使用者輸入之一使用者帳號及一演算式，送出一確認視窗，該確認視窗至少包含隨機產生一種子字串提示給該用戶端電腦供確認該演算式；

(c) 回應來自該使用者輸入之依該演算式而將該種子字串轉換成作為密碼之第一串字串，該電腦裝置比較依該演算式轉換該種子字串所得之第二串字串與該第一串字串以確認該演算式；以及

（d）回應該確認，儲存該帳號及該演算式。

參考以下說明及隨附申請專利範圍或利用如下文所提之本發明的實施方式，即可更加明瞭本發明的這些特色及優點。

【實施方式】

本說明書中「一具體實施例」或類似表達方式的引用是指結合該具體實施例所述的特定特色、結構、或特性係包括在本發明的至少一具體實施例中。因此，在本說明書中，「在一具體實施例中」及類似表達方式之用語的出現未必指相同的具體實施例。

熟此技藝者當知，本發明可實施為電腦裝置、方法或作為電腦程式產品之電腦可讀媒體。因此，本發明可以實施為各種形式，例如完全的硬體實施例、完全的軟體實施例（包含韌體、常駐軟體、微程式碼等），或者亦可實施為軟體與硬體的實施形式，在以下會被稱為「電路」、「模組」或「系統」。此外，本發明亦可以任何有形的媒體形式實施為電腦程式產品，其具有電腦可使用程式碼儲存於其上。

一個或更多個電腦可使用或可讀取媒體的組合都可以利用。舉例來說，電腦可使用或可讀取媒體可以是（但並不限於）電子的、磁的、光學的、電磁的、紅外線的或半導體的系統、裝置、

設備或傳播媒體。更具體的電腦可讀取媒體實施例可以包括下列所示（非限定的例示）：由一個或多個連接線所組成的電氣連接、可攜式的電腦磁片、硬碟機、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM 或快閃記憶體)、光纖、可攜式光碟片（CD-ROM）、光學儲存裝置、傳輸媒體（例如網際網路(Internet)或內部網路(intranet)之基礎連接）、或磁儲存裝置。需注意的是，電腦可使用或可讀取媒體更可以為紙張或任何可用於將程式列印於其上而使得該程式可以再度被電子化之適當媒體，例如籍由光學掃描該紙張或其他媒體，然後再編譯、解譯或其他合適的必要處理方式，然後可再度被儲存於電腦記憶體中。在本文中，電腦可使用或可讀取媒體可以是任何用於保持、儲存、傳送、傳播或傳輸程式碼的媒體，以供與其相連接的指令執行系統、裝置或設備來處理。電腦可使用媒體可包括其中儲存有電腦可使用程式碼的傳播資料訊號，不論是以基頻(baseband)或是部分載波的型態。電腦可使用程式碼之傳輸可以使用任何適體的媒體，包括（但並不限於）無線、有線、光纖纜線、射頻(RF)等。

用於執行本發明操作的電腦程式碼可以使用一種或多種程式語言的組合來撰寫，包括物件導向程式語言（例如 Java、Smalltalk、C++或其他類似者）以及傳統程序程式語言（例如 C 程式語言或其他類似的程式語言）。程式碼可以獨立軟體套件的形式完整的於使用者的電腦上執行或部分於使用者的電腦上執行，或部分於使用者電腦而部分於遠端電腦。

於以下本發明的相關敘述會參照依據本發明具體實施例

之電腦裝置、方法及電腦程式產品之流程圖及／或方塊圖來進行說明。當可理解每一個流程圖及／或方塊圖中的每一個方塊，以及流程圖及／或方塊圖中方塊的任何組合，可以使用電腦程式指令來實施。這些電腦程式指令可供通用型電腦或特殊電腦的處理器或其他可程式化資料處理裝置所組成的機器來執行，而指令經由電腦或其他可程式化資料處理裝置處理以便實施流程圖及／或方塊圖中所說明之功能或操作。

這些電腦程式指令亦可被儲存在電腦可讀取媒體上，以便指示電腦或其他可程式化資料處理裝置來進行特定的功能，而這些儲存在電腦可讀取媒體上的指令構成一製成品，其內包括之指令可實施流程圖及／或方塊圖中所說明之功能或操作。

電腦程式指令亦可被載入到電腦上或其他可程式化資料處理裝置，以便於電腦或其他可程式化裝置上進行一系統操作步驟，而於該電腦或其他可程式化裝置上執行該指令時產生電腦實施程序以達成流程圖及／或方塊圖中所說明之功能或操作。

其次，請參照圖 2 至圖 7B，在圖式中顯示依據本發明各種實施例的電腦裝置、方法及電腦程式產品可實施的架構、功能及操作之流程圖及方塊圖。因此，流程圖或方塊圖中的每個方塊可表示一模組、區段、或部分的程式碼，其包含一個或多個可執行指令，以實施指定的邏輯功能。另當注意者，某些其他的實施例中，方塊所述的功能可以不依圖中所示之順序進行。舉例來說，兩個圖示相連接的方塊事實上亦可以同時執

行，或依所牽涉到的功能在某些情況下亦可以依圖示相反的順序執行。此外亦需注意者，每個方塊圖及／或流程圖的方塊，以及方塊圖及／或流程圖中方塊之組合，可籍由基於特殊目的硬體的系統來實施，或者籍由特殊目的硬體與電腦指令的組合，來執行特定的功能或操作。

<電腦裝置>

圖 2 說明本發明之例示性服務提供者伺服器 202 之硬體環境方塊圖。在一個示範性的實施例中，伺服器為一台通用型之桌上型電腦，可具有處理器以執行各種應用程式；儲存裝置以儲存各種資訊及程式碼；顯示裝置、通訊及輸出/入裝置做為與使用者溝通之介面；以及週邊元件或其他特定用途元件。在其他實施例中，本發明亦可實施為其他的形式，而具有更多或更少之其他裝置或元件。網路亦可實施為任何型式之連線，包括固定連接之區域網路(LAN)或廣域網路(WAN)連線，或利用網際網路服務提供者來暫時撥接至網際網路，亦不限於有線無線等各種連接方式，例如透過 GSM、或 Wi-Fi 等無線網路與用戶端電腦通信。然而應了解，雖未繪示但其他硬體及軟體組件(例如額外電腦系統、路由器、防火牆等)可包含於網路之中。

如圖 2 所示，伺服器 202 包括一耦合至系統匯流排 206 之處理器單元 204。一視訊配接器 208(其控制一顯示器 210)亦耦合至系統匯流排 206。系統匯流排 206 藉由一匯流排橋 212 耦合至一輸入/輸出(I/O)匯流排 214。一 I/O 介面 216 耦合至 I/O 匯流排 214。I/O 介面 216 能與各個 I/O 裝置之

通信，該等 I/O 裝置包括一鍵盤 218、一滑鼠 220、一唯讀光碟機(CD-ROM)222、一軟碟機 224 及一快閃記憶體隨身碟 226。I/O 裝置更可為數位相機模組用以輸入影像資料或是條碼資料，或是 I/O 裝置可與顯示器 210 整合為觸控螢幕，用以供使用者操作應用程式與編寫資訊。連接到 I/O 介面 216 之埠的規格，可以是熟悉電腦架構技術者所知之任一種，其包括(但不限於)通用串列匯流排(USB)埠。

使用一網路介面 230，伺服器 202 能藉由一網路 228 與一用戶端電腦 252 通信，網路介面 230 耦合至系統匯流排 206。網路 228 可係一外部網路(例如，網際網路)或一內部網路(例如，一乙太網路或一虛擬私人網路(VPN))。使用網路 228，伺服器 202 能使用本發明以與用戶端電腦 252 互動。

一硬碟機介面 232 亦耦合至系統匯流排 206 上。硬碟機介面 232 與一硬碟機 234 介接。在一較佳實施例中，硬碟機 234 進駐（populates）系統記憶體 236，該系統記憶體 236 亦耦合至系統匯流排 206。進駐系統記憶體 236 之資料包括伺服器 202 之作業系統(OS)238 及應用程式 244。

OS 238 包括一用於供使用者存取諸如應用程式 244 等資源之殼層(shell)240 及核心 242。殼層 240 係一可在使用者與作業系統間提供一解譯器與介面的程式。該殼層提供系統提示、解譯由鍵盤、滑鼠或其他使用者輸入媒體所輸入的命令及向該作業系統之適當的較低層級(例如，核

心 242)發送經解譯之命令供進行處理。雖然殼層 240 一般係以文字為基礎之行導向式使用者介面，但本發明亦能支援其他使用者介面模式，諸如圖形的、語音的、示意動作的模式等。核心 242 包括 OS 238 之較低層級功能，該等較低層級功能包括由 OS 238 之其他部分及應用程式 244 所要求之基本服務，該基本服務包括：記憶體管理、處理序及任務管理、磁碟管理及滑鼠與鍵盤之管理。

用戶端電腦252可以使用與前述伺服器202相同或類似的硬體架構，亦或者可以利用其他的基礎架構，本發明並不限制。舉例來說，用戶端電腦可以是桌上型電腦、筆記型電腦、個人數位助理(PDA)、智慧型手機等。然而圖 2 所示以及上述的範例皆非用於限制本發明的架構。用戶端電腦 252 可包括一瀏覽器。瀏覽器包括程式模組及指令，該等程式模組及指令使用超文字傳送協定(HTTP)訊息使全球資訊網(WWW)用戶端(即：用戶端電腦 252)能夠發送及接收網路訊息至網際網路，因此實現與伺服器 202 通信。

應用程式 244 可包括一本發明之密碼式盤問模組 246。密碼式盤問模組 246 包括程式模組及指令，該等程式模組及指令能與用戶端電腦 252 通信，以識別使用者身份。該密碼式盤問模組 246 可以是應用程式內之模組，或以常駐程式(Daemon)之方式實施。但在其他實施例中，亦可以用其他形式之程式型態來實施。 該密碼式盤問模組 246 包括用於實施下文所說明之圖 4A 及 4B 內所說明之程

序之代碼。

在伺服器 202 內繪示之硬體元件並非意欲包羅萬象，而係代表本發明所使用之最重要元件。舉例而言，伺服器 202 可以另包括替代記憶體儲存裝置，諸如磁帶(magnetic cassette)、多樣化數位光碟(DVD)、(Bernoulli)卡匣及類似者。此等及其它變化將包含在本發明之精神及範疇內

<密碼/盤問鑑定流程>

圖 4A 與圖 4B 係配合圖 3 以顯示伺服器 202 端密碼式盤問模組的方法步驟。圖 5 與圖 6 係配合圖 4A 以顯示伺服器提示之登錄與確認（verification）之執行畫面。

圖 4A 為一種依據本發明一具體實施例之密碼/盤問鑑定之登錄（registration）的方法流程圖。

- 步驟 400: 伺服器 202 端接收一來自用戶端電腦 252 存取一網務服務之請求。
- 步驟 402: 回應該請求，伺服器 202 送出一登錄網頁 500（如圖 5 所示）。該用戶端電腦 252 之使用者輸入帳號且在該登錄網頁 500 上建立其想要的演算式。
- 步驟 404:回應該用戶端電腦 252 使用者之完成輸入演算式，伺服器 202 端送出一確認網頁 600（如圖 6 所示）並隨機產生一種子字串提示給該用戶端電腦 252 使用者供確認該演算式。使用者再輸入依該使用者記住之演算式將該種子字串轉換為作為密碼之第一串字串。

- 步驟 406: 伺服器 202 將再利用該使用者輸入之該演算式轉換該種子字串所得之第二串字串與使用者輸入之第一串字串作比較。若相同，則確認成功。回應該成功，伺服器 202 儲存該帳號及該演算式。

圖 5 所示之登錄網頁 500 可包含演算式所需之轉換運算子 510，運算元 Which 520、運算元 Where 530 及邏輯運算子 AND 540。轉換運算子 510 可包含 Move、Append 、Convert、Add_、Sub_及 Square 等等，但本發明並不侷限於此。

運算元 Which 520 指示種子字串中哪些字串要被轉換運算子轉換，例如，整個字串(All)、僅有字元（Character）、僅有數字（Number）、僅有字母（Alphabet）、僅有大寫字母（Upper Case）、僅有小寫字母（Lower Case）、第"_"字串（The "_"th） 、最先第"_"符號（The first "_"symbol） 、最後第"_" 符號（The last "_"symbol）及一組固定字串（或簡稱"字組"）（Pattern_）等等，但本發明並不侷限於此。其中"_"代表數字。

運算元 Where 530 指示種子字串中那些要被轉換運算子轉換之字串需被轉換到的位置或方式，例如，頭部(Head)、尾部（Tail）、轉換為大寫字母（Upper Case）、轉換為小寫字母（Lower Case）、轉換為數字（Numeric number）、轉換為字母（Alphabet letter）、轉換至第"_"位置（The "_"th place）、及轉換為一"字組"（Pattern_）等等，但本發明並不侷限於此。

依據本發明之具體實施例，使用者輸入帳號的網頁（未顯示）與要建立其想要演算式之登錄網頁是不同網頁。但本發明並不侷限於此，在其他不同實施例，輸入帳號的網頁與登錄網頁可以是相同網頁。

如前述，該用戶端電腦252之使用者輸入帳號且在該登錄網頁 500 上使用前述轉換運算子 510，運算元 Which 520、運算元 Where 530 及邏輯運算子 AND 540，建立其想要的演算式公式 550。此外，藉由增加符 560，使用者可建立包含一組公式之演算式。當使用者完成其想要的演算式後，可進入一確認網頁 600 進行該演算式之確認。

圖6所示之確認網頁600可包含使用者建立之包含一組公式之演算式 610 及一確認區 620 等等，但本發明並不侷限於此。該確認區 620 包含一種子字串區，一密碼輸入區，一伺服器 202 利用該使用者輸入之該演算式轉換該種子字串所得之第二串字串顯示區及一比對結果區。例如，伺服器 202 隨機產生一第一串字串"6kq3U&;1"，經利用該使用者輸入之該演算式 610 轉換後，獲得一第二串字串"LOL@35kq8U;0XD"。即依該演算式 610 第一式，將種子字串中所有數字取平方再減一；第二式將種子字串中第一個符號（此例為"&"）轉換為"XD"並移至種子字串之尾部；最後，第二式將字組"LOL@" 移至種子字串之頭部。

該種子字串區包含3個伺服器202隨機產生之種子字串供使用者確認該演算式。至於該種子字串區包含之種子

字串的數目可為任意，本發明並不欲設限。至於該種子字串只是利用一般隨機產生技術獲得，如：網址(http://www.random.org/strings/)所述之 Random String Generator。本發明係提供字串作為種子，因而也適用於使用終端機登入伺服器的環境。本發明也可提供習知"CAPTCHA"影像作為種子供使用者利用，至於"CAPTCHA"影像請參見習知"CAPTCHA"影像之相關產生技術，在此不予贅述。

圖 4B 為一種依據本發明一具體實施例之密碼/盤問鑑定之登入（login）的方法流程圖；圖 4B 係配合圖 3 以顯示伺服器 202 端之方法步驟。圖 3 為一種依據本發明一具體實施例之密碼/盤問鑑定之系統示意圖。

- 步驟 410: 伺服器 310 端回應接收一來自用戶端電腦 300 存取一網務服務之登入請求，送出一登入網頁 700（如圖 7A 所示）。該登入網頁 700 包含伺服器 310 隨機產生之種子字串顯示欄 710，帳號輸入欄 720 及密碼輸入欄 730。
- 步驟 412: 伺服器 310 回應使用者輸入之帳號，送出一隨機產生之顯示在該種子字串顯示欄 710 之一種子字串 301。伺服器 310 也可於回應接收一來自一用戶端電腦存取一網務服務之登入請求時，同時送出一包含隨機產生之一種子字串及一帳號輸入欄的登入網頁。
- 步驟 414: 伺服器 310 回應使用者輸入依該使用者記住之演算式而將該種子字串轉換成作為密碼之第一串字串 303（即 f(種子)）及使用者帳號，伺服器 310 依該儲存之與該

使用者帳號相關之演算式轉換該種子字串所得之正確密碼（第二串字元）（即 F(種子)）與使用者輸入的密碼（即第一串字元，f(種子)）作比較。若相同（即 f(種子)= F(種子)），則登入成功。

- 步驟 416: 若登入失敗，伺服器 310 可再送出一登入網頁 700'（如圖 7B 所示）。重複步驟 412 及步驟 414 之步驟。

需說明的是，依本發明揭示者，使用者與伺服器間共享的是使用者建立之演算式，而非需定期更改之密碼。在網路上傳輸的密碼是依演算式計算而得的結果，其只有一次有效。因此，縱使密碼被暴露，駭客也不能在使用它。因而，本發明不需再定期更改之密碼。此外，使用者可對所有網站使用該演算式，而不再需記住許多用來登入不同網站以存取網路服務的不同密碼。因此，本發明有習知 OTP 的優點，而無其需要一電子裝置之缺點。

此外，本發明也可適用於一般非使用網路之各式各樣的資訊裝置，例如行動電話、個人電腦、筆記型電腦、平板電腦等，其中因皆儲存有使用者的個人資料及身分資料，因此也可利用本發明之密碼式盤問模組，而提供單機之應用。該密碼式盤問模組 246 可以是應用程式內之模組，但在其他實施例中，亦可以用其他形式之程式型態來實施，例如整合入作業系統層次供啟動作業系統時盤問使用者。

在不脫離本發明精神或必要特性的情況下，可以其他特定形式來體現本發明。應將所述具體實施例各方面僅視為解說

性而非限制性。因此，本發明的範疇如隨附申請專利範圍所示而非如前述說明所示。所有落在申請專利範圍之等效意義及範圍內的變更應視為落在申請專利範圍的範疇內。

【圖式簡單說明】

為了立即瞭解本發明的優點，請參考如附圖所示的特定具體實施例，詳細說明上文簡短敘述的本發明。在瞭解這些圖示僅描繪本發明的典型具體實施例並因此不將其視為限制本發明範疇的情況下，參考附圖以額外的明確性及細節來說明本發明，圖式中：

圖 1 為一種習知密碼/盤問鑑定之系統示意圖；

圖 2 為本發明之例示性服務提供者伺服器 202 之硬體環境方塊圖；

圖 3 一為種依據本發明一具體實施例之密碼/盤問鑑定之系統示意圖；

圖 4A 與圖 4B 分別為一種依據本發明一具體實施例之密碼/盤問鑑定之登錄（registration）與登入（login）的方法流程圖；

圖 5 顯示本發明實施例中登錄之執行畫面；

圖 6 顯示本發明實施例中確認（verification）之執行畫面；

圖 7A 與圖 7B 顯示本發明實施例中登入之執行畫面。

【主要元件符號說明】

100 客戶端

101 盤問

102 帳號/密碼

110、120、130 網站 A、網站 B、網站 C

140 網路

202 服務提供者伺服器

204 處理器單元

206 系統匯流排

208 視訊配接器

210 顯示器

212 匯流排橋

214 輸入/輸出(I/O)匯流排

216 I/O 介面

218 鍵盤

220 滑鼠

222 唯讀光碟機(CD-ROM)

224 軟碟機

226 快閃記憶體隨身碟

228 網路

230 網路介面

232 硬碟機介面

234 硬碟機

236 系統記憶體

238 作業系統(OS)

240 殼層(shell)

242 核心

244 應用程式

246 密碼式盤問模組

252 用戶端電腦

300 用戶端電腦

301 種子字串

303 第一串字串

310 伺服器

七、申請專利範圍：

1. 一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該用戶端電腦之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該用戶端電腦之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

2. 一種在一伺服器中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之登入請求，送出一登入網頁；該登入網頁至少包含隨機產生之一種子字串及一帳號輸入欄；以及

(b)回應來自該用戶端電腦之一使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

3. 一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視

窗；該登入視窗至少包含一顯示隨機產生之一種子字串的顯示欄及一帳號輸入欄；

(b)回應來自該使用者輸入之一使用者帳號，送出一隨機產生之顯示在該種子字串顯示欄之一種子字串；以及

(c)回應來自該使用者之該使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

4. 一種在一電腦裝置中動態提供演算式密碼/盤問鑑定的方法，該方法包含:

(a) 回應接收一來自一使用者之登入請求，送出一登入視窗；該登入視窗至少包含隨機產生之一種子字串及一帳號輸入欄；以及

(b)回應來自該使用者輸入之一使用者帳號及依一演算式而將該種子字串轉換成作為密碼之第一串字串，比較依該事先已儲存而與該使用者帳號相關之演算式轉換該種子字串所得之第二串字串與該第一串字串。

5. 一種在一伺服器中登錄一密碼式盤問之演算式的方法，該方法包含:

(a) 回應接收一來自一用戶端電腦存取一網務服務之請求，送出一登錄網頁，該登錄網頁至少包含建立演算式所需之複數個轉換運算子，複數個運算元及一邏輯運算子；

(b) 回應來自該用戶端電腦之一使用者帳號及一演算式，送出一確認網頁，該確認網頁至少包含隨機產生一種子字串提

示給該用戶端電腦供確認該演算式；

(c) 回應來自該用戶端電腦之依該演算式而將該種子字串轉換成作為密碼之第一串字串，該伺服器比較依該演算式轉換該種子字串所得之第二串字串與該第一串字串以確認該演算式；以及

(d) 回應該確認，儲存該帳號及該演算式。

6. 一種在一電腦裝置中登錄一密碼式盤問之演算式的方法，該方法包含:

(a) 回應接收一來自一使用者存取一網務服務之請求，送出一登錄視窗，該登錄視窗至少包含建立演算式所需之複數個轉換運算子，複數個運算元及一邏輯運算子；

(b) 回應來自該使用者輸入之一使用者帳號及一演算式，送出一確認視窗，該確認視窗至少包含隨機產生一種子字串提示給該用戶端電腦供確認該演算式；

(c) 回應來自該使用者輸入之依該演算式而將該種子字串轉換成作為密碼之第一串字串，該電腦裝置比較依該演算式轉換該種子字串所得之第二串字串與該第一串字串以確認該演算式；以及

(d) 回應該確認，儲存該帳號及該演算式。

7. 如請求項 5 或 6 之方法，其中該複數個運算元至少包含一第一運算元指示該種子字串中哪些字串要被該複數個轉換運算子轉換，及一第二運算元指示該種子字串中那些要被該複數個轉換運算子轉換之字串需被轉換到的位置或方式；

其中，該第一運算元至少包含整個字串(All)、僅有字元（Character）、僅有數字（Number）、僅有字母（Alphabet）、僅有大寫字母（Upper Case）、僅有小寫字母（Lower Case）、第”_”字串（The “_” th）、最先第”_”符號（The first “_” symbol）、最後第”_” 符號(The last “_” symbol)及一組固定字串（或簡稱”字組”）（Pattern_）中之一者；及

其中，該第二運算元至少包含頭部(Head)、尾部（Tail）、轉換為大寫字母（Upper Case）、轉換為小寫字母（Lower Case）、轉換為數字（Numeric number）、轉換為字母（Alphabet letter）、轉換至第”_”位置（The “_” th place）、及轉換為一”字組”（Pattern_）中之一者；其中，該”_”代表數字。

8. 一種動態提供演算式密碼/盤問鑑定的伺服器，包含：

一主機；該主機包含，

一匯流排系統；

一記憶體，連接到該匯流排系統，其中該記憶體包含一組指令；

一連接到該匯流排系統之處理單元，其中該處理單元執行該組指令，以執行如申請專利範圍第 1 至 7 項之任一項所述之方法。

9. 一種儲存在一電腦可用媒體上之電腦程式產品，包含一電腦可讀程式，供於一電腦上執行時，以實施如申請專利範圍第 1 至 7 項之任一項所述之方法，以在一伺服器中動態提供演算式密碼/盤問鑑定。

10. 一種提供一介面供一使用者操作以動態提供演算式密碼/盤問鑑定的伺服器，包含：

一主機；該主機包含，

一匯流排系統；

一記憶體，連接到該匯流排系統，其中該記憶體包含一組指令；

一連接到該匯流排系統之處理單元，其中該處理單元執行該組指令，以執行如申請專利範圍第 1 至 7 項之任一項所述之方法。