(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2009 年2 月12 日 (12.02.2009)

PCT

(10) 国际公布号
WO 2009/018685 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
G06F 21/00 (2006.01)

(21) 国际申请号: PCT/CN2007/002384

(22) 国际申请日: 2007 年8 月8 日 (08.08.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人及
(72) 发明人: **黄金富(WONG, Kamfu)** [CN/CN]; 中国香港特别行政区沙田径口路3号金富台, Hong Kong (CN)。

(74) 代理人: **中国专利代理（香港）有限公司(CHINA PATENT AGENT (H.K.) LTD.)**; 中国香港特别行政区湾仔港湾道23号鹰君中心22号楼, Hong Kong (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告。

(54) Title: THE DEVICE AND THE METHOD OF ENCRYPTING AND AUTHENTICATING AGAINST TROJAN HORSE WITH ONE TIME KEY

(54) 发明名称: 对抗木马程式用完即弃一次性密钥的加密认证装置和方法

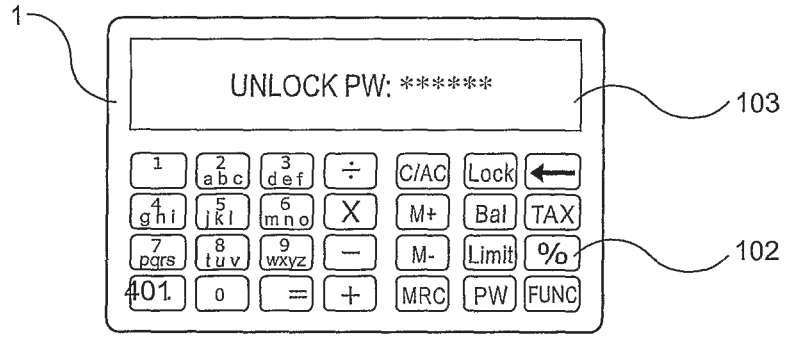

图1 / Fig. 1

(57) Abstract: The device, the system and the method of encrypting and authenticating against Trojan horse includes the following steps, the user information including the password, the sum of the transaction, and the number of the account is inputted using the keyboard (102). The user information is encrypted by the key (A), and is sent to the server (4) through the user device (2) and the network (3). The server decrypts the received information with the key (B). Because the key (A) used each time has no relations with other key (A), the information is safe even if it is obtained by the hacker in the process of being transmitted. At the same time, the information is inputted through the keyboard (102) of the device of the encrypting and authenticating (1). The hacker can not obtain the information inputted through the keyboard (102) of the device of the encrypting and authenticating (1) even if the Trojan horse invades into the user's computer.

[见续页]

WO 2009/018685 A1

(57) 摘要：

一种可对抗木马程式的加密认证装置及相应系统和方法，采用一次性密钥作为加密和认证，并设有键盘（102）供用户输入资料，包括用户口令、交易金额、账户号码等资料，然后以密钥（A）将资料加密，再通过终端机（2）经网络（3）传送给服务器（4），由服务器（4）使用相配对的密钥（B）将资料解密还原出用户所输入的资料。即使资料在传输过程被黑客截取了，由于资料是采用用完即弃的一次性密钥加密，每条密钥（A）与其他密钥（A）之间是没有关连，令黑客无法破解，加上资料是从加密认证装置（1）的键盘（102）上输入，即使黑客采用木马程式入侵用户的计算机，也无法读取用户在加密认证装置（1）的键盘（102）上输入的资料。

对抗木马程式用完即弃一次性密钥的加密认证装置和方法

【技术领域】

本发明涉及信息传送安全领域，特别是涉及一种用于认证的加密认证装置和相应认证方法。

【背景技术】

随着时代的进步，资讯科技的应用非常普及，尤其是金融机构如银行等，提供了很多利用资讯科技的服务，例如网上银行服务、手机银行服务、网上证券买卖服务等，这些服务一般是将用户的交易信息通过网络传送到金融机构，由金融机构核实用户的交易信息后，根据信息内容进行相应的操作。

由于现时一般网络的安全性问题，经常会发生黑客盗用他人账户的事件，故此有些金融机构采用一些双因素认证手段来对抗黑客，例如采用保安编码器（Token Device），用户登入金融机构的服务器时，由保安编码器产生一个编码，用户除了要输入正确的用户口令外，还要输入正确的编码才能登入金融机构的服务器。这些保安编码器一般内置有一条密钥，使用时由保安编码器根据时间等因素，通过复杂的算法计算产生一个保安编码，而在金融机构的服务器内也采用相同的一条密钥，根据时间等因素通过相同的算法计算产生一个编码，如果金融机构的服务器所产生的编码与接收到由保安编码器所产生的保安编码相同，就可认证该保安编码器的身份，加上核对用户口令，要同时通过保安编码和用户口令的认证，才能成功登入。这种双因素认证手段虽然可以改善网络安全的问题，但仍然有部

份网络保安问题未妥善解决，例如一些黑客采用各种入侵方法，将木马程式置于用户的计算机内，在用户连线到金融机构的服务器时，通过木马程式盗取用户的资料，包括账户号码、账户口令和用户输入的保安编码等，有些黑客甚至制造一个伪冒的金融机构的网站，欺骗用户在伪冒的金融机构的网站输入交易资料，然后黑客根据盗取到资料，即时登入金融机构的服务器，继而盗取用户账户内的钱。

此外，随着计算机技术的发展，计算机的运算能力越来越强，一些从前被认为是安全可靠不可破解的信息加密措施，也可能通过拥有强大运算能力的计算机所破解，令采用这些信息加密措施的金融机构的安全性受到重大挑战，为了保障用户账户的安全，很多金融机构采用了更复杂的密钥和算法的加密解密技术，令经营成本增加，而且随着计算机技术的发展，只要数年时间，在目前被视为安全可靠的信息加密措施也可能被全面破解，令金融机构和用户面对相当大的风险，所以很多人都不敢使用金融机构的网上交易服务，这是一个极待解决的问题。

【发明内容】

本发明的目的，在于提供一种加密认证装置，用于认证用户的身份和交易资料。

本发明的目的是这样实现的，采用这样一种加密认证装置，用于身份认证，其特征在于，所述的加密认证装置(1)的主要结构包括有主芯片(101)、键盘（102）、显示屏（103）、通讯接口（104），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现认证用户在服务器（4）的身份和各项预定功能，包括将资料加密、储存资料、

通过键盘（102）读取用户输入的资料、通过显示屏（103）显示提示信息、通过通讯接口（104）发送认证资料给服务器（4），以及，加密认证装置（1）将用户通过键盘（102）输入的资料，包括用户口令、操作指令、账户号码等资料，以密钥（A）将资料加密，再通过终端机（2）和网络（3）传送给服务器（4），由服务器（4）使用相配对的密钥（B）将资料解密还原出用户所输入的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器（4）才会根据资料内容进行相应的操作；以及，主芯片（101）内还包括有一个唯一的装置编号（105）和多条密钥（A）和多个索引号（C），每一个索引号（C）对应一条密钥（A），以及，各个索引号（C）是互不相同的。

本发明的加密认证装置（1），是采用用完即弃一次性的密钥（A）作为加密和认证手段，并且在加密认证装置（1）上设置有键盘（102）供用户输入资料，包括用户口令、操作指令、账户号码等资料，然后以密钥（A）将资料加密，再通过终端机（2）经网络（3）传送给服务器（4），由服务器（4）使用与该密钥（A）相配对的密钥（B）将资料解密还原出用户口令、操作指令、账户号码等资料，这样在传输过程中即使被黑客截取了资料，由于资料已经加密，而且是采用用完即弃的密钥（A）加密，每条密钥（A）与其他密钥（A）之间是没有关连的，令黑客无法破解，加上资料是从加密认证装置（1）的键盘（102）上输入，加密认证装置（1）与用户的计算机之间是物理上分离的，即使黑客采用木马程式入侵用户的计算机，木马程式也无法读取加密认证装置（1）的键盘（102）上的按键输入的资料。

在设置方面，服务器（4）内设有多个认证账户（401），每一个认证账户（401）对应一个加密认证装置（1），认证账户（401）内储存有该账户

所对应的加密认证装置（1）的装置编号（105）和一个账户密码，每一认证账户（401）内储存有多条密钥（B）和多个索引号（C），每一个索引号（C）对应一条密钥（B），以及，每一认证账户（401）内的密钥（B）与该账户的加密认证装置（1）内的密钥（A）成配对关系，每一条密钥（B）有一条相配对的密钥（A），每一对相配对的密钥（A）和密钥（B）它们所对应的索引号（C）是相同的。使用本发明的加密认证装置（1）前，要预先由服务器（4）通过各种方法随机方式产生多对密钥和多个顺序的索引号（C），每一对密钥分配一个索引号（C），然后将每一对密钥分别连同所分配的索引号（C）储存到加密认证装置（1）的主芯片（101）和认证账户（401）内，储存到主芯片（101）的称为密钥（A），而储存到认证账户（401）的称为密钥（B），如果采用的加密算法是非对称密码算法，密钥（A）和密钥（B）就是一对互相配对的密钥，如果采用的加密算法是对称密码算法，密钥（A）和密钥（B）就是一对相同的密钥，当使其中一条密钥（A）将资料加密后，可以使用与该密钥（A）相配对的密钥（B）将资料解密。

本发明的另一特征是，加密认证装置（1）的主芯片（101）每次将资料加密时，会按预定程序从主芯片（101）内提取一条未用的密钥（A）将资料加密，以及，主芯片（101）将资料加密后，就会将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（101）使用。以及，服务器（4）每次将资料解密时，会按预定程序从认证账户（401）内提取一条与该资料相配对的密钥（B）将资料解密，以及，服务器（4）将资料解密后，就会将该条密钥（B）删除或弃置或标记为已用，使该条密钥（B）不会再次被服务器（4）使用。

以及，采用这样一种加密认证电讯系统，用于用户身份认证用途，特别用于金融业，包括采用前面所述的加密认证装置（1）、终端机（2）、网络（3）、服务器（4），其中，加密认证装置（1）独立于终端机（2），与终端机（2）相分离设置，本系统中各加密认证装置（1）分别在服务器（4）内登记及被服务器（4）所识别，在加密认证装置（1）和服务器（4）内分别设有相配对的密钥（A，B），加密过程在加密认证装置（1）中进行，利用密钥（A）形成密文，经终端机（2）及网络（3）传输至服务器（4），服务器（4）利用相配对的密钥（B）解密密文，解密成功则识别成功，所述系统进入后面预定程序。

以及，采用这样一种加密认证方法，采用前面所述的加密认证装置，用于身份认证等用途，其特征在于，所述的方法包括用户使用终端机（2）登入服务器（4）时，用户预先在加密认证装置（1）上输入账户密码等需要认证的资料，由加密认证装置（1）将需要认证的资料加密为密文，然后通过终端机（2）经网络（3）将该密文传送到服务器（4），由服务器（4）将密文解密还原出需要认证的资料，服务器（4）核对需要认证的资料无误后，用户的身份认证成功，可以登入服务器（4）。

这样就实现了本发明的目的。

本发明的加密认证装置（1）的优点是每条密钥只会使用一次，用完即弃，不会重复使用，使黑客不能从加密后的资料中破解出密钥或资料内容，而且加密认证装置（1）上设有键盘（102）供用户输入重要资料，即使黑客采用木马程式入侵用户的计算机，也无法盗取用户输入的重要资料，特别适合于网上银行、网上交易等应用范围。

【附图说明】

图 1 是本发明的加密认证装置（1）的形像化示意说明图；

图 2 是本发明的加密认证装置（1）的另一外形的形像化示意说明图；

图 3 是具备 USB 接口（104）的加密认证装置（1）的形像化示意说明图；

图 4 是具备英文键盘（102）的加密认证装置（1）的形像化示意说明图；

图 5 是本发明的加密认证装置（1）的方框结构说明图；

图 6 是本发明的加密认证装置（1）的与服务器（4）在使用时的步骤示意说明图。

图中，相同的数字代表相同的系统、装置、部件器件，方法步骤用圆圈的数字和带箭头的直线所标出。附图是示意性的，用以说明本发明的加密认证装置（1）的主要特征和使用时的操作步骤。

【具体实施方式】

下面结合附图，对本发明的方法作进一步详细说明。

参阅图 1 至图 4，图 1 是本发明的加密认证装置（1）的形像化示意说明图，图 2 是本发明的加密认证装置（1）的另一外形的形像化示意说明图，图 3 是具备 USB 接口（104）的加密认证装置（1）的形像化示意说明图，图 4 是具备英文键盘（102）的加密认证装置（1）的形像化示意说明图，图 1 至图 4 中示出了加密认证装置（1）不同外形的实施方式的形像化示意说明图，图中示出的加密认证装置(1)除了外形不相同外，它们的键盘(102)按键也有分别，加密认证装置（1）的键盘（102）可以是包含数字按键的键盘（102）、或包含英文字母按键的键盘（102）、或包含数字和英文字母的键盘（102）。

参阅图 5，图 5 是本发明的加密认证装置（1）的方框结构说明图，图中示出的加密认证装置（1）的主要结构包括有主芯片（101）、键盘（102）、显示屏（103）、通讯接口（104），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现认证用户在服务器（4）的身份和各项预定功能，包括将资料加密、储存资料、通过键盘（102）读取用户输入的资料、通过显示屏（103）显示提示信息、通过通讯接口（104）发送认证资料给服务器（4），以及，加密认证装置（1）将用户通过键盘（102）输入的资料，包括用户口令、操作指令、账户号码等资料，以密钥（A）将资料加密，再通过终端机（2）和网络（3）传送给服务器（4），由服务器（4）使用相配对的密钥（B）将资料解密还原出用户所输入的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器（4）才会根据资料内容进行相应的操作；以及，主芯片（101）内还包括有一个唯一的装置编号（105）和多条密钥（A）和多个索引号（C），每一个索引号（C）对应一条密钥（A），以及，各个索引号（C）是互不相同的。

继续参阅图 5，图中示出的通讯接口（104）可以是无线通讯装置、或有线通讯装置、或蓝芽装置、或红外线装置、或 USB 接口、或 SD 记忆卡接口、或 MINI-SD 记忆卡接口、或 MMC 记忆卡接口、或 RS-MMC 记忆卡接口、或 RS-232 接口、或 PS2 键盘接口。

参阅图 6，图 6 是本发明的加密认证装置（1）与服务器（4）在使用时的步骤示意说明图，图中示出的服务器（4）内设有多个认证账户（401），每一个认证账户（401）对应一个加密认证装置（1），认证账户（401）内储存有该账户所对应的加密认证装置（1）的装置编号（105）和一个账户密码，每一认证账户（401）内储存有多条密钥（B）和多个索引号（C），

每一个索引号（C）对应一条密钥（B），以及，每一认证账户（401）内的密钥（B）与该账户的加密认证装置（1）内的密钥（A）成配对关系，每一条密钥（B）有一条相配对的密钥（A），每一对相配对的密钥（A）和密钥（B）它们所对应的索引号（C）是相同的。密钥（A）和密钥（B）是由服务器（4）预先通过各种方法随机方式产生，当密钥（A）储存到加密认证装置（1）的主芯片（101）后，只有主芯片（101）才能对密钥（A）作内部访问，而不允许任何外部的访问，以保证密钥（A）的安全。

此外，加密认证装置（1）的主芯片（101）每次将资料加密时，会按预定程序从主芯片（101）内提取一条未用的密钥（A）将资料加密，以及，主芯片（101）将资料加密后，就会将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（101）使用。以及，服务器（4）每次将资料解密时，会按预定程序从认证账户（401）内提取一条与该资料相配对的密钥（B）将资料解密，以及，服务器（4）将资料解密后，就会将该条密钥（B）删除或弃置或标记为已用，使该条密钥（B）不会再次被服务器（4）使用。由于密钥（A）和密钥（B）是用完即弃的，每一条密钥只会使用一次，当加密认证装置（1）内的密钥（A）全部用完后，加密认证装置（1）就不能继续使用，用户必须更换新的加密认证装置（1），如果加密认证装置（1）内储存有 1 万条密钥（A），以平均每天使用 10 次计算，大约可以使用 3 年。

在加密解密算法方面，密钥(A)和密钥(B)是采用一次性密码(One Time Pad 或称为 Vernam-cipher），所谓一次性密码是通过使用与讯息一样长的随机生成的密钥，将密钥与讯息进行位元的“XOR”运算产生密文，解密时应用同一密钥和适当的演算法，就可以方便地解密还原出讯息，由于密钥

只使用一次，然后就被丢弃，所以是无法破解的，是最简单安全和快速的加密算法。本发明的加密认证装置（1）除了可以采用一次性密码（One Time Pad）加密算法外，也可以采用其他的加密算法，也可很好地实现本发明的目的，可以采用的加密算法包括：

1. 数据加密标准（Data Encryption Standard - DES）；

2. 三重数据加密标准（Triple - DES）；

3. RSA 加密演算法（RSA algorithm）；

4. 一次性密码（One Time Pad）；

5. 公钥基础架构（Public Key Infrastructure - PKI）。

本发明的加密认证装置（1）的主芯片（101）将资料加密前，被加密的资料内容还包括有校验资料，以保障资料不会被窜改，所述的校验资料是由被加密的资料通过包括如下其中之一的校验算法所产生：

1. 循环冗余码（CRC）算法；

2. 摘要演算法（Message-Digest Algorithm）；

3. 消息认证码（Message authentication code）算法；

4. 安全杂凑标准（Secure Hash Standard）算法。

以及，在服务器（4）将加密资料解密后，服务器（4）采用相同的校验算法就可检测资料有没有被窜改。

更进一步，还可以采用开机口令保护加密认证装置（1）不会被盗用，即在加密认证装置（1）的主芯片（101）还设有开机口令，每次使用加密认证装置（1）前，使用者必须通过键盘（102）输入正确的开机口令，才能使用加密认证装置（1）进行各项操作。

在本说明书中，服务器（4）是指供用户登入的各类计算机主机，服务器（4）可以是各金融机构的账户服务器、或银行账户系统服务器、或任何需要验证用户身份合法性的计算机等，而终端机（2）是指与服务器（4）相连线的终端设备，可以是计算机、或计算机终端、或 ATM 机等需要认证用户身份的终端设备，通过本发明的加密认证装置（1），就能可靠地验证登入服务器（4）的用户身份的合法性。

继续参阅图 6，图中示出包括如下的步骤，是用户登入服务器（4）时，通过加密认证装置（1）进行认证的步骤，具体的步骤如下：

1. 用户使用终端机（2）通过网络（3）连线到服务器（4），在加密认证装置（1）的键盘（102）上输入账户密码等资料，加密认证装置（1）内的主芯片（101）将用户输入的资料和装置编号（105）通过预定的校验算法计算出包含校验资料的认证资料，然后在主芯片（101）内提取一条未用的密钥（A）将认证资料加密为密文，并提取出该密钥（A）所对应的索引号（C），主芯片（101）将认证资料加密后将该条密钥（A）删除或弃置或标记为已用；
2. 加密认证装置（1）通过显示屏（103）将密文连同索引号（C）显示给用户看，然后用户在终端机（2）上输入登入名称、显示屏（103）所显示的密文内容和索引号（C）等资料；

   或；

   用户在终端机（2）上输入登入名称，然后将加密认证装置（1）的通讯接口（104）与终端机（2）连接，将密文连同索引号（C）通过通讯接口（104）传送到终端机（2）；

3. 终端机（2）通过网络（3）将登入名称、密文和索引号（C）传送到服务器（4）；

4. 服务器（4）从登入名称找到用户的认证账户（401），从索引号（C）在该认证账户（401）内提取对应该索引号（C）的密钥（B）将密文解密还原出认证资料，服务器（4）将密文解密后将该条密钥（B）删除或弃置或标记为已用，并通过预定的校验算法校验认证资料和还原出装置编号（105）和账户密码等资料，校验无误后表示认证资料没有被窜改过，服务器（4）核对装置编号（105）和账户密码等资料无误后，表示用户的身份认证成功，然后服务器（4）通过网络（3）向终端机（2）发出信息，通知用户已经成功登入了服务器（4）。

在本实施例步骤中，为了方便用户查看显示屏（103）所显示的内容，可将密文连同索引号（C）以每四个字符一组的方式在显示屏（103）上显示，在字符组与字符组之间以一个空格或“-”作分隔，方便用户查看显示内容，可减少用户因看错内容而出错。

本发明的加密认证装置（1）和认证方法安全可靠，用户可通过加密认证装置（1）上的键盘（102）输入重要资料，即使黑客采用木马程式入侵用户的计算机，最多只能盗取用户在计算机键盘输入的资料，黑客是无法盗取用户在加密认证装置（1）输入的重要资料。本发明的实施，会带来巨大的良好的社会效益。

权利要求

1. 一种加密认证装置，用于身份认证，其特征在于，所述的加密认证装置（1）的主要结构包括有主芯片（101）、键盘（102）、显示屏（103）、通讯接口（104），其中，主芯片（101）内设有 CPU 和存储器，并与其它各部件相连接，按预定程序运作，实现认证用户在服务器（4）的身份和各项预定功能，包括通过键盘（102）读取用户输入的资料、储存资料、加密资料、通过显示屏（103）显示提示信息、通过通讯接口（104）发送认证资料给服务器（4）；

以及，

加密认证装置（1）将用户通过键盘（102）输入的资料，包括用户口令、操作指令、账户号码等资料，以密钥（A）将资料加密，再通过终端机（2）和网络（3）传送给服务器（4），由服务器（4）使用相配对的密钥（B）将资料解密还原出用户所输入的资料，并核对资料内容，核对无误后表示用户的身份认证成功，然后服务器（4）才会根据资料内容进行相应的操作。

2. 如权利要求 1 所述的加密认证装置，其特征在于，所述的主芯片（101）内还包括有一个唯一的装置编号（105）和多条密钥（A）和多个索引号（C），每一个索引号（C）对应一条密钥（A），以及，各个索引号（C）是互不相同的。

3. 如权利要求 2 所述的加密认证装置，其特征在于，所述的主芯片（101）每次将资料加密时，会按预定程序从主芯片（101）内提取一条未用的密钥（A）将资料加密，以及，主芯片（101）将资料加密后，就会将该条密钥（A）删除或弃置或标记为已用，使该条密钥（A）不会再次被主芯片（101）使用。

4. 如权利要求 1 所述的加密认证装置，其特征在于，所述的主芯片（101）还设有开机口令，每次使用加密认证装置（1）前，使用者必须通过键盘（102）输入正确的开机口令，才能使用加密认证装置（1）进行各项操作。

5. 如权利要求 1 或 2 或 3 或 4 所述的加密认证装置，其特征在于，所述的主芯片（101）将资料加密时，可以采用包括如下的其中之一的加密算法：

1. 数据加密标准（Data Encryption Standard - DES）；
2. 三重数据加密标准（Triple - DES）；
3. RSA 加密演算法（RSA algorithm）；
4. 一次性密码（One Time Pad）；
5. 公钥基础架构（Public Key Infrastructure - PKI）。

6. 如权利要求 1 或 2 或 3 或 4 所述的加密认证装置，其特征在于，所述的主芯片（101）将资料加密前，被加密的资料内容还包括有校验资料，以保障资料不会被窜改。

7. 如权利要求 6 所述的加密认证装置，其特征在于，所述的校验资料是由被加密的资料通过包括如下其中之一的校验算法所产生：

1. 循环冗余码（CRC）算法；

2. 摘要演算法（Message-Digest Algorithm）；

3. 消息认证码（Message authentication code）算法；

4. 安全杂凑标准（Secure Hash Standard）算法。

8. 如权利要求 1 所述的加密认证装置，其特征在于，所述的通讯接口（104）可以是无线通讯装置、或有线通讯装置、或蓝芽装置、或红外线装置、或 USB 接口、或 SD 记忆卡接口、或 MINI-SD 记忆卡接口、或 MMC 记忆卡接口、或 RS-MMC 记忆卡接口、或 RS-232 接口、或 PS2 键盘接口。

9. 一种加密认证电讯系统，用于用户身份认证用途，特别用于金融业，包括采用如权利要求 1-8 所述加密认证装置（1），以及终端机（2）、网络（3）、服务器（4），其中，加密认证装置（1）独立于终端机（2），与终端机（2）相分离设置，本系统中各加密认证装置（1）分别在服务器（4）内登记及被服务器（4）所识别，在加密认证装置（1）和服务器（4）内分别设有相配对的密钥（A，B），加密过程在加密认证装置（1）中进行，利用密钥（A）形成密文，经终端机（2）及网络（3）传输至服务器（4），服务器（4）利用相配对的密钥（B）解密密文，解密成功则识别成功，所述系统进入后面预定程序。

10. 如权利要求 9 所述的加密认证电讯系统，其特征在于，所述的服务器（4）内设有多个认证账户（401），每一个认证账户（401）对应一个加密认证装置（1），认证账户（401）内储存有该账户所对应的加密认证装置（1）的装置编号（105）和一个账户密码，每一认证账户（401）内储存有多条密钥（B）和多个索引号（C），每一个索引号（C）对应一条密钥（B），

以及，

每一认证账户（401）内的密钥（B）与该账户的加密认证装置（1）内的密钥（A）成配对关系，每一条密钥（B）有一条相配对的密钥（A），每一对相配对的密钥（A）和密钥（B）它们所对应的索引号（C）是相同的。

11. 如权利要求 9 所述的加密认证电讯系统，其特征在于，所述的服务器（4）每次将资料解密时，会按预定程序从认证账户（401）内提取一条与该资料相配对的密钥（B）将资料解密，以及，服务器（4）将资料解密后，就会将该条密钥（B）删除或弃置或标记为已用，使该条密钥（B）不会再次被服务器（4）使用。

12. 一种加密认证方法，采用如权利要求 1 至 10 任一项所述的加密认证装置，用于身份认证等用途，其特征在于，所述的方法包括用户使用终端机（2）登入服务器（4）时，用户预先在加密认证装置（1）上输入账户密码等需要认证的资料，由加密认证装置（1）将需要认证的资料加密为密文，然后通过终端机（2）经网络（3）将该密文传送到服务

器（4），由服务器（4）将密文解密还原出需要认证的资料，服务器（4）核对需要认证的资料无误后，用户的身份认证成功，可以登入服务器（4）。

13. 如权利要求 12 所述的加密认证方法，用于身份认证等用途，其特征在于，所述的方法包括如下的步骤，是用户登入服务器（4）时，通过加密认证装置（1）进行认证的步骤，具体的步骤如下：

1. 用户使用终端机（2）通过网络（3）连线到服务器（4），在加密认证装置（1）的键盘（102）上输入账户密码等资料，加密认证装置（1）内的主芯片（101）将用户输入的资料和装置编号（105）通过预定的校验算法计算出包含校验资料的认证资料，然后在主芯片（101）内提取一条未用的密钥（A）将认证资料加密为密文，并提取出该密钥（A）所对应的索引号（C），主芯片（101）将认证资料加密后将该条密钥（A）删除或弃置或标记为已用；
2. 加密认证装置（1）通过显示屏（103）将密文连同索引号（C）显示给用户看，然后用户在终端机（2）上输入登入名称、显示屏（103）所显示的密文内容和索引号（C）等资料；

   或；

   用户在终端机（2）上输入登入名称，然后将加密认证装置（1）的通讯接口（104）与终端机（2）连接，将密文连同索引号（C）通过通讯接口（104）传送到终端机（2）；
3. 终端机（2）通过网络（3）将登入名称、密文和索引号（C）传送到服务器（4）；

4. 服务器（4）从登入名称找到用户的认证账户（401），从索引号（C）在该认证账户（401）内提取对应该索引号（C）的密钥（B）将密文解密还原出认证资料，服务器（4）将密文解密后将该条密钥（B）删除或弃置或标记为已用，并通过预定的校验算法校验认证资料和还原出装置编号（105）和账户密码等资料，校验无误后表示认证资料没有被窜改过，服务器（4）核对装置编号（105）和账户密码等资料无误后，表示用户的身份认证成功，然后服务器（4）通过网络（3）向终端机（2）发出信息，通知用户已经成功登入了服务器（4）。

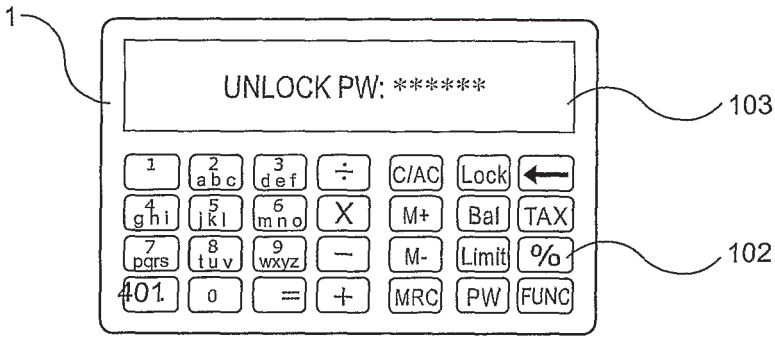

图 1

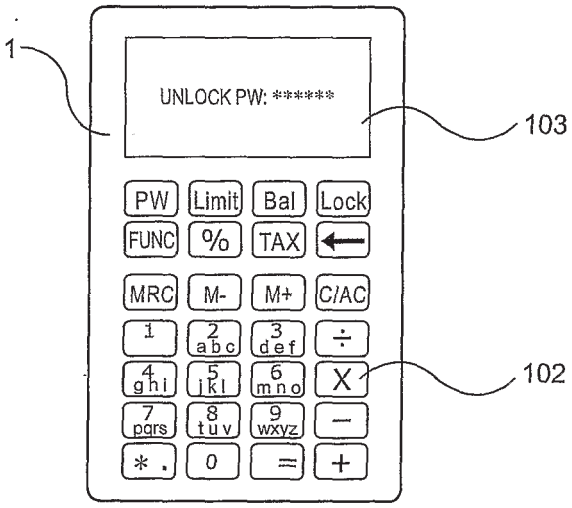

图 2

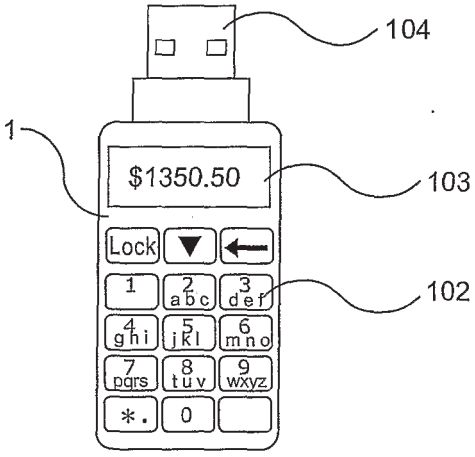

图 3

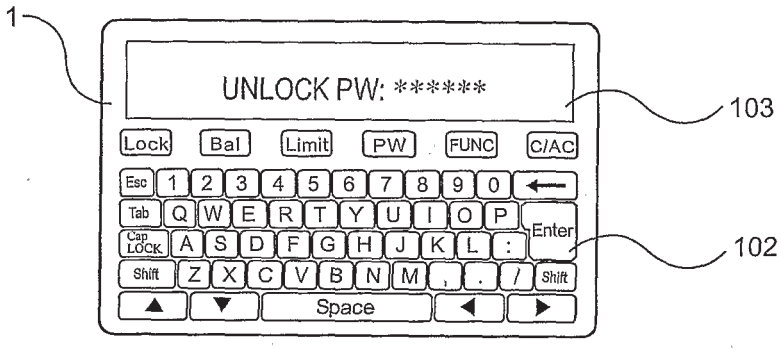
1
UNLOCK PW: ******
103
Lock
Bal
Limit
PW
FUNC
C/AC
Esc
Tab
Cap LOCK
Shift
Enter
102
Space

图 4

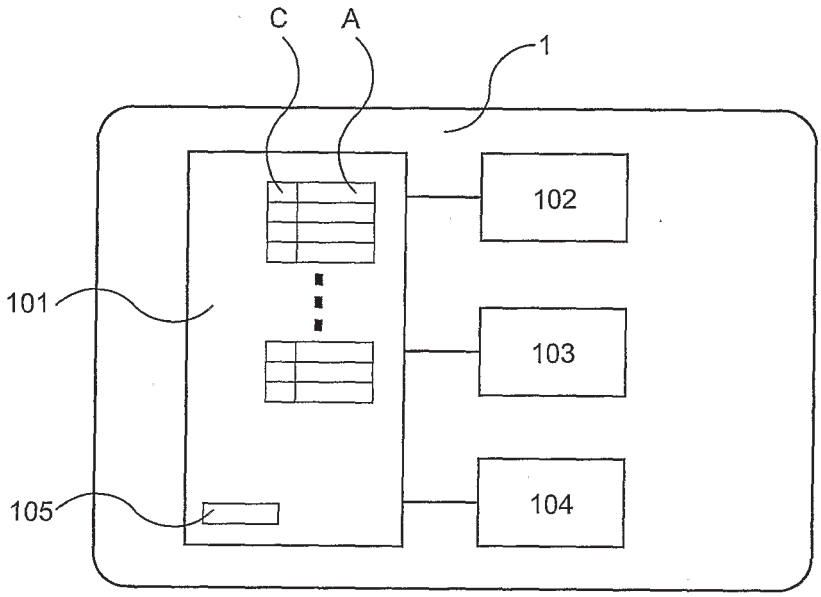
C
A
1
102
101
103
104
105

图 5

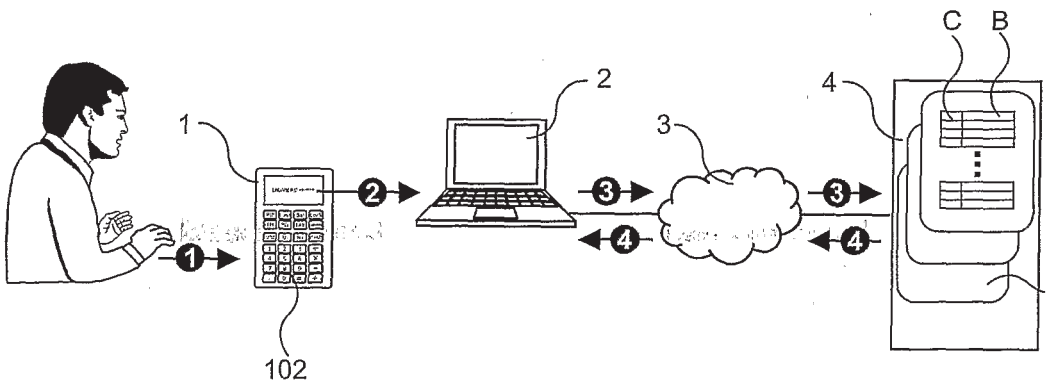
C
B
2
4
1
3
102

图 6