(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1981476 B
(45)授权公告日 2012.07.04

(21)申请号 200580022256.1

(22)申请日 2005.04.18

(30)优先权数据
0411560.6 2004.05.24 GB

(85)PCT申请进入国家阶段日
2006.12.30

(86)PCT申请的申请数据
PCT/GB2005/001479 2005.04.18

(87)PCT申请的公布数据
WO2005/117331 EN 2005.12.08

(73)专利权人 吉科瑞普有限公司
地址 英国伦敦

(72)发明人 M·阿尔库拉姆卜瑞

(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民 薛峰

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 2003172262 A1,2003.09.11, 全文.
EP 0869652 A2,1998.10.07, 全文.
CN 1249096 A,2000.03.29, 全文.
CN 1189949 A,1998.08.05, 全文.
US 2003046533 A1,2003.03.06, 全文.

审查员 刘冀鹏

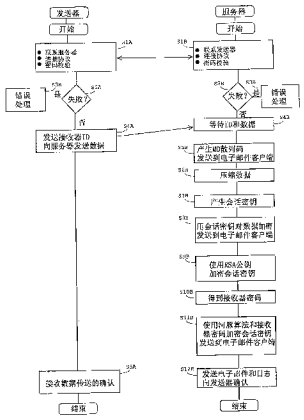
权利要求书 2 页 说明书 10 页 附图 4 页

(54)发明名称

一种使用网络在发送器和接收器之间加密并传送数据的方法

(57)摘要

本发明涉及一种使用网络在发送器和接收器之间加密并传送数据的方法，因此能以安全方式传送数据。该方法包括以下步骤：服务器从发送器接收接收器的标识符(S4A，S4B)；建立专用于所述传送的传送专用加密密钥(S7B)；用所述传送专用加密密钥对数据进行加密(S8B)；服务器根据接收到的接收器的标识符，访问接收器专用信息，并用接收器专用信息对所述传送专用加密密钥进行加密(S11B)；通过网络传送加密的数据和加密的传送专用加密密钥，以便由接收器接收(S11B)；服务器从接收器接收加密的传送专用加密密钥；服务器访问接收器专用信息以对加密的传送专用加密密钥进行解密；并使用解密的传送专用加密密钥对加密的数据进行解密。



CN 1981476 B

1. 一种使用网络在发送器和接收器之间加密和传送数据的方法，所述方法包括以下步骤：

一服务器从发送器接收接收器的标识符；

生成专用于所述发送器和所述接收器之间的相应数据传送的传送专用加密密钥；

使用所生成的传送专用加密密钥对要传送的数据进行加密；

所述服务器根据从所述发送器接收到的所述接收器的所述标识符重新得到被访问的接收器专用信息，并且利用所重新得到的接收器专用信息对所生成的传送专用加密密钥进行加密；

通过所述网络传送加密的数据和加密的传送专用加密密钥，以便由所述接收器接收；

所述服务器从所述接收器接收所述加密的传送专用加密密钥和所述接收器的标识符，其中所述加密的数据和所述加密的传送专用加密密钥已经传送到所述接收器；

所述服务器根据从所述接收器接收到的所述接收器的所述标识符重新得到被访问的所述接收器专用信息，并利用所重新得到的接收器专用信息对所述加密的传送专用加密密钥进行解密；和

使用解密的传送专用加密密钥对所述加密的数据进行解密。

2. 根据权利要求 1 所述的方法，进一步包括在所述发送器和所述服务器之间建立通信链路，并将所述接收器的所述标识符发送到所述服务器。

3. 根据权利要求 2 所述的方法，进一步包括在所述发送器和所述服务器之间建立所述通信链路，使其为安全链路。

4. 根据权利要求 2 所述的方法，进一步包括在所述发送器和服务器之间建立所述通信链路，由所述服务器校验所述发送器的密码。

5. 根据权利要求 1 所述的方法，进一步包括在所述接收器和所述服务器之间建立通信链路，并将所述接收器的所述标识符发送到所述服务器。

6. 根据权利要求 5 所述的方法，进一步包括在所述接收器和所述服务器之间建立所述通信链路，使其为安全链路。

7. 根据权利要求 5 所述的方法，进一步包括在所述接收器和所述服务器之间建立所述通信链路，由所述服务器校验所述接收器的密码。

8. 根据权利要求 1 所述的方法，其中生成所述传送专用加密密钥发生在所述发送器上，且所生成的传送专用加密密钥被发送到所述服务器。

9. 根据权利要求 1 所述的方法，其中使用所述传送专用加密密钥对数据进行加密发生在所述发送器上。

10. 根据权利要求 9 所述的方法，其中所述发送器从所述服务器接收所述加密的传送专用加密密钥，且所述发送器通过网络将所述加密的数据和所述加密的传送专用加密密钥传送到所述接收器。

11. 根据权利要求 1 所述的方法，其中所述接收器从所述服务器接收所述解密的传送专用加密密钥，且使用所述解密的传送专用加密密钥对所述加密的数据进行解密发生在所述接收器上。

12. 根据权利要求 1 所述的方法，其中生成所述传送专用加密密钥发生在所述服务器上。

13. 根据权利要求 12 所述的方法，其中使用所述传送专用加密密钥对所述数据进行加密发生在所述服务器上。

14. 根据权利要求 13 所述的方法，其中所述服务器通过网络向所述接收器传送所述加密的数据和所述加密的传送专用加密密钥。

15. 根据权利要求 1 所述的方法，其中使用所述解密的传送专用加密密钥对所述加密的数据进行解密发生在所述服务器上，且所述服务器将所解密的数据传送到所述接收器。

16. 根据权利要求 1 所述的方法，进一步包括：

在加密之前，为所述数据生成消息认证码 (MAC) 值；

与所述加密的数据和所述加密的传送专用加密密钥一起传送所述 MAC 值；和

在解密之后，为所述数据生成 MAC 值，并对照所传送的 MAC 值对其进行验证。

17. 根据权利要求 1 所述的方法，其中加密所述传送专用加密密钥使用了公钥加密方法、河豚算法、以及所述服务器的保密码中的一种或多种。

18. 一种对服务器进行操作以使用网络在发送器和接收器之间加密并传送数据的方法，所述方法包括以下步骤：

从发送器接收接收器的标识符；

根据从所述发送器接收到的所述接收器的所述标识符重新得到被访问的接收器专用信息，并利用所重新得到的接收器专用信息对传送专用加密密钥进行加密，所述传送专用加密密钥专用于所述发送器和所述接收器之间相应的数据传送并且用于加密要传送的数据；

在已通过网络传送加密的数据和加密的传送专用加密密钥到所述接收器之后，从所述接收器接收所述加密的传送专用加密密钥和所述接收器的标识符；和

根据从所述接收器接收到的所述接收器的所述标识符重新得到被访问的所述接收器专用信息，并利用所重新得到的接收器专用信息对所述加密的传送专用加密密钥进行解密。

19. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括在所述服务器中生成一个专用于所述传送的传送专用加密密钥。

20. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括从所述发送器接收专用于所述传送的传送专用加密密钥；

并向所述发送器传送所述加密的传送专用加密密钥。

21. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括使用所述传送专用加密密钥对所述服务器中的所述数据进行加密。

22. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括通过所述网络传送所述加密的数据和所述加密的传送专用加密密钥以由所述接收器接收。

23. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括向所述接收器传送所解密的传送专用加密密钥。

24. 根据权利要求 18 所述的对服务器进行操作的方法，进一步包括使用所解密的传送专用加密密钥对所述服务器中的所述加密的数据进行解密。

一种使用网络在发送器和接收器之间加密并传送数据的方法

技术领域

[0001] 本发明涉及一种使用网络在发送器(sender)和接收器(receiver)之间加密并传送数据的方法，因此能以安全的方式传送数据。

背景技术

[0002] 目前，敏感数据正日益以电子形式从发送器发送到接收器。在这种情况下，确保数据不被截取或不被没有授权的人读取就变得越来越重要了，也就是说，必须以安全的方式传送数据以使数据的内容仅能被发送器和接收器访问。

[0003] 在一种情况下，在进行数据传送前，可在发送器A和接收器B之间建立安全连接链路。然而，在一些情况下，比如说一个办公室中10个人希望互相通信并在它们中间传送敏感数据并以双向方式将数据传送到另一个远处的办公室中的10个人，布置如此多的安全连接链路需要额外的硬件和软件，因此存在许多缺点。此外，要维持这种链接及该链接相关的密码系统涉及大量的硬件资源和时间资源。当每一个办公室中的人员通过一些形式的企业内联网或以太网连接在一起及通过因特网办公通信时，尤为如此。需要发送器和接收器两端有复杂的加密和解密软件，这需要另外的硬件和软件系统，及相关的专门维护费用。

[0004] 在另一种情况下，希望用单个发送器将不同的数据传送到多个分立的接收器。然而，这种情况与上述提到的情况具有相同的缺点。特别地，对发送器而言，需要建立复杂的安全条款以保持密码系统安全。而且，必须建立额外的硬件和软件系统以存储和维持这种系统。

[0005] 实际上，在诸如个人数字助理，具有因特网接入和电子邮件功能的移动电话的小型手持设备时代，由于它们具有有限的存储空间和处理能力，要使这些设备建立包括高级的加密和解密的双向安全连接在技术上通常是不可行的。

[0006] 尽管可以使用数字认证来减少服务器和接收器对技术资源的需求，但通常涉及对接收器而言不合理的费用，即使当该费用较少时。

[0007] 对发送器而言，一种替代性方法是对要传送的数据进行加密，然后通过网络发送加密的数据。然而，接收器还是必须具有可用的硬件处理资源及相关软件的存储空间，以便能够对加密的数据进行解密。而且，在接收器的设备具有相对较弱的硬件资源的情况下，占用宝贵的资源以能安全地传送数据通常是不可行的。

[0008] 使用复杂的加密和解密技术需要在发送器的设备和接收器的设备上安装特定的软件。这既不方便又很昂贵。而且，安装程序既复杂又耗时，并可能与各自设备上的其它软件冲突。更进一步，额外的软件可能需要一定的处理能力，这在设备上是不可用的，并且会占用宝贵的存储器空间；这对上述的手持设备尤为如此。

[0009] 根据以上内容可清楚地看出，以安全方式传送数据的已知方法和系统需要大量的安装配置以及大量的计算机处理和本地存储器资源。对那些仅有有限的上述技术资源的设备的发送器和/或接收器的情况而言，显然是不合理的。

[0010] 因此，需要一种以安全方式传送数据的方法和系统，其能减少发送器和 / 或接收器设备所要求的技术资源级别。而且，在使用公钥 / 私钥加密的情况下，发送器必须确信它们认为属于接收器的公钥未被闯入者的公钥代替。

发明内容

[0011] 根据本发明的一个方面，提供了一种使用网络在发送器和接收器之间加密和传送数据的方法，所述方法包括以下步骤：一服务器从所述发送器接收所述接收器的标识符；建立专用于所述传送的传送专用加密密钥；使用所述传送专用加密密钥对所述数据进行加密；所述服务器根据接收到的所述接收器的标识符来访问接收器专用信息，并且利用所述接收器专用信息，对所述传送专用加密密钥进行加密；通过所述网络传送加密的数据和加密的传送专用加密密钥，以便由所述接收器接收；所述服务器从所述接收器接收所述加密的传送专用加密密钥；所述服务器访问所述接收器专用信息，以对所述加密的传送专用加密密钥进行解密；和使用解密的传送专用加密密钥对所述加密的数据进行解密。

[0012] 优选为，所述方法进一步包括在所述发送器和所述服务器之间建立通信链路，并将所述接收器的所述标识符发送到所述服务器。

[0013] 在一个实施例中，所述方法进一步包括在所述发送器和所述服务器之间建立所述通信链路，使其为安全链路。

[0014] 在一种情况下，所述方法进一步包括在所述发送器和服务器之间建立通信链路，由所述服务器校验所述发送器的密码。

[0015] 在另一个实施例中，所述方法进一步包括在所述接收器和所述服务器之间建立通信链路，并将所述接收器的所述标识符发送到所述服务器。

[0016] 在一种情况下，所述方法进一步包括在所述接收器和所述服务器之间建立所述通信链路，使其为安全链路。

[0017] 在一种特定情况下，所述方法进一步包括在所述接收器和服务器之间建立所述通信链路，由所述服务器校验所述接收器的密码。

[0018] 优选为，建立所述传送专用加密密钥发生在所述发送器上，且所建立的传送专用加密密钥被发送到所述服务器。

[0019] 在另一种情况下，使用所述传送专用加密密钥对数据进行加密发生在所述发送器上。

[0020] 在一个特定的实施例中，所述发送器从所述服务器接收所述加密的传送专用加密密钥，且所述发送器通过网络将所述加密的数据和所述加密的传送专用加密密钥传送到所述接收器。

[0021] 在另一个实施例中，所述接收器从所述服务器接收所述解密的传送专用加密密钥，而使用所述解密的传送专用加密密钥对所述加密的数据进行解密发生在所述接收器上。

[0022] 在又一个实施例中，建立所述传送专用加密密钥发生在所述服务器上。

[0023] 在一种特定的情况下，使用所述传送专用加密密钥对所述数据进行加密发生在所述服务器上。

[0024] 在一个实施例中，所述服务器通过网络向所述接收器传送所述加密的数据和所述

加密的传送专用加密密钥。

[0025] 在另一实施例中，使用所述解密的传送专用加密密钥对所述加密的数据进行解密发生在所述服务器上，且所述服务器将所述解密的数据传送到所述接收器。

[0026] 优选为，所述方法进一步包括将所述接收器的标识符从所述发送器发送到所述服务器。

[0027] 在另一个实施例中，所述方法进一步包括将所述接收器的标识符从所述接收器发送到所述服务器。

[0028] 更便利地，所述方法进一步包括：在加密之前，为所述数据建立消息认证码 (MAC) 值；与所述加密的数据和所述加密的传送专用加密密钥一起传送所述 MAC 值；和在解密之后，为所述数据建立 MAC 值，并对照所传送的 MAC 值对齐进行验证。

[0029] 在一个实施例中，加密所述传送专用加密密钥使用了公钥加密方法、河豚算法、以及服务器保密码中的一种或多种。

[0030] 根据本发明的另一方面，提供了一种对服务器进行操作以使用网络在发送器和接收器之间加密并传送数据的方法，所述方法包括以下步骤：从所述发送器接收所述接收器的标识符；根据接收到的所述接收器的标识符来访问接收器专用信息，并利用所述接收器专用信息对用于加密所述数据的传送专用加密密钥进行加密；在已通过网络传送加密的数据和加密的传送专用加密密钥以便由所述接收器接收之后，从所述接收器接收所述加密的传送专用加密密钥。访问所述接收器专用信息，以对所述加密的传送专用加密密钥进行解密。

[0031] 在一个实施例中，所述对服务器进行操作的方法进一步包括在所述服务器中建立一个专用于所述传送的传送专用加密密钥。

[0032] 在另一个实施例中，所述对服务器进行操作的方法进一步包括从所述发送器接收专用于所述传送的传送专用加密密钥；并向所述发送器传送所述加密的传送专用加密密钥。

[0033] 优选为，所述对服务器进行操作的方法进一步包括使用所述传送专用加密密钥对所述服务器中的所述数据进行加密。

[0034] 在另一个优选的实施例中，所述对服务器进行操作的方法进一步包括通过所述网络传送所述加密的数据和所述加密的传送专用加密密钥以由所述接收器接收。

[0035] 优选为，所述对服务器进行操作的方法进一步包括向所述接收器传送所述解密的传送专用加密密钥。

[0036] 在另一个实施例中，所述对服务器进行操作的方法进一步包括使用所述解密的传送专用加密密钥对所述服务器中的所述加密的数据进行解密。

[0037] 根据本发明的另一方面，提供了一种计算机媒介，其用于使用网络在发送器和接收器之间加密和传送数据的方法，所述媒介包括：用于从所述发送器接收所述接收器的标识符，并建立专用于所述传送的传送专用加密密钥的计算机码；用于使用所述传送专用加密密钥对所述数据进行加密的计算机码；根据所述接收到的所述接收器的标识符访问接收器专用信息，并用所述接收器专用信息对所述传送专用加密密钥进行加密的计算机码；用于通过所述网络传送所述加密的数据和所述加密的传送专用加密密钥以由所述接收器接收的计算机码；用于从所述接收器接收所述加密的传送专用加密密钥并用于访问所述接收

器专用信息以对所述加密的传送专用加密密钥进行解密的计算机码；和用于使用所述解密的传送专用加密密钥对所述加密的数据进行解密的计算机码。

附图说明

[0038] 现在将参考附图对本发明的一个例子进行描述，附图中：

[0039] 图 1 示出了一个系统的示意图，该系统运行了本发明的使用网络在发送器和接收器之间加密和传送数据的方法；

[0040] 图 2 示出了用在图 1 中的服务器的运行模块的示意性方框图；

[0041] 图 3 是一个流程图，其示出了包括在发送器和接收器中用于本发明从发送器向服务器发送数据的处理过程；

[0042] 图 4 是一个流程图，其示出了包括在发送器和接收器中响应从服务器接收到的电子邮件的处理过程。

具体实施方式

[0043] 现参考图 1 和图 2，它们所示为运行使用网络在发送器和接收器之间加密和传送数据的方法的一个实施例的系统。参考这两个图，所述系统运行以在发送器设备 100 和接收器设备 200 之间加密和传送数据。

[0044] 在此例中，发送器设备 100 包括连接到键盘 107，数据源 108 和外部显示设备 105 的计算机 101。数据源包括某些类型的磁盘阅读器或连接到数据库的接口，所述数据源存储要传送给接收器的数据。计算机 101 具有通用访问总线 106，该通用访问总路线连接到微处理器 102，存储器 103，显示器接口 104，输入设备接口 109，和通过连接 111 接连到因特网的网络浏览器 110。

[0045] 显示器接口 104 连接到外部显示设备 105，同时输入设备接口 109 接连到键盘 107 和数据源 108。存储器 103 通常存储发送器的 ID 和发送器的密码，尽管发送器的 ID 和密码可能是响应显示设备 105 上的显示提示通过键盘 107 的输入。

[0046] 在此例中，接收器设备 200 包括通过网络浏览器 210 经由连接 211 连接到因特网的具有因特网能力的移动电话。关于如何建立这种连接的详细情况是本领域公知的，在此不做描述。网络浏览器连接到通用访问总线 206，该通用访问总线 206 连接到微处理器 202，存储器 203，显示器接口 204 和输入设备接口 209。显示器接口 204 连接到集成显示设备 205，同时输入设备接口 209 连接到集成键盘 207。存储器 203 一般存储接收器的 ID 和接收器的密码，尽管接收器的 ID 和密码可能是响应显示设备 205 上的显示提示通过键盘 207 的输入。设备 200 进一步包括电子邮件客户端 212 以用于通过连接 213 连接到因特网来发送和接收电子邮件。

[0047] 服务器 300 也通过连接 302 连接到因特网上。服务器结构的详细方框图如图 2 所示。结合对本发明的系统运行的描述来对服务器的这种结构进行解释。

[0048] 参考图 1 和图 2，在使用本系统前，发送器和接收器两者最初都注册到服务器 300 上。它们的详细情况存储在服务器数据库模块 306 内。在本实施例中，对每一发送器和接收器而言，存储的信息包括至少一个 ID 和一个密码。

[0049] 发送器希望将保持在数据源 108 中的数据传送给接收器。为了使发送器传送数

据，发送器需要知道接收器的 ID 和服务器 300 的网络地址。此信息可以存储在发送器的存储器 103 中或可以人为地通过键盘 107 输入以响应显示设备 105 上的提示。

[0050] 如图 2 所示，服务器 300 包括通过连接 302 连接到因特网的网络服务器 301。网络服务器连接到输入总线 303 并由微处理器 304 控制。当发送器联系服务器的网络地址时，就建立了诸如加密套接字协议层 (SSL) 链接的安全链路，其详细情况为本领域熟练技术人员所公知。微处理器 304 不允许发送器访问本系统直到模块 305 完成密码验证并访问数据库模块 306。这种密码验证的详情为本领域所公知，因此这里不作描述。

[0051] 密码验证完成后，服务器 300 向发送器发出屏幕显示。完成该屏幕后，发送器向服务器发送接收器 ID 的身份和从数据源 108 得到的要传送的数据。朝向图上边缘的模块作用于这些输入。

[0052] 一旦接收到接收器的 ID 和发送的数据，服务器微处理器 304 将数据发送到消息认证码 (MAC) 发生器模块 307。这种发生器产生的一组编码是使用部分或全部数据并结合加密摘要算法的计算得到的，其为本领域公知。在这种情况下，使用已知的消息摘要 (MD) 散列算法来从此数据中生成一个 MD 散列值。MD 散列值发送到通过链路 316 连接到因特网的邮件客户端 312，以准备好处理成电子邮件的一部分。

[0053] 接收到的数据在模块 308 中压缩后，由模块 309 使用从模块 310 得到的会话密钥进行加密。本领域公知，会话密钥是从随机数发生器 311 产生的随机数中产生的。此会话密钥专用于此数据及此数据的传送，因此成为了一种传送专用加密密钥。之后，加密的数据发送到准备好处理成电子邮件一部分的电子邮件客户端 312。

[0054] 也使用公钥 / 私钥加密技术的公钥，诸如本领域公知的 RSA 加密，对来自模块 310 的会话密钥在模块 313 中进行加密。之后，模块 313 的输出在模块 314 中使用河豚 (blowfish) 算法进一步加密，其合并了从数据库 306 得到的接收器的密码。该密码是根据从微处理器发送的在总线 315 上的接收器的 ID 的输出。加密的会话密钥发送到准备好处理成电子邮件一部分的电子邮件客户端 312。

[0055] 电子邮件客户端 312 以已知的方式处理 MD 散列值，加密的数据和加密的会话密钥以构成一个电子邮件然后将其发送到由总线 315 上的微处理器访问数据库 306 之后提供的合适的接收器地址。电子邮件客户端以已知的方式向电子邮件分配一特有的标签并记录发送它的标志。使用网络服务器 301 或电子邮件客户端 312 将电子邮件发送的确认信息发送到发送器。

[0056] 由服务器 300 发送的电子邮件可以以一般的方式由移动电话 200 的电子邮件客户端 212 接收。建立电子邮件的内容以提示接收器使用本发明的系统传送数据或自动激活网络浏览器 210 以初始化服务器 300 的通信链路。在任何一种情况下，在微处理器 202 的控制下，当接收器联系服务器的网络地址时，就建立了诸如 SSL 链接的安全链路，其详细情况为本领域熟练技术人员所公知。服务器的微处理器 304 不允许访问本系统直到模块 305 完成密码验证并访问数据库模块 306。这种密码验证的详情为本领域所公知，因此这里不作描述。

[0057] 只有密码校验成功完成之后，包含在电子邮件中的加密的数据，加密的会话密钥和 MD 散列值才会通过网络服务器 301 在服务器 300 的安全链接上发送。朝向图的下边的模块作用于其上。

[0058] 很显然如果选择的发送和读取电子邮件的方法是通过网络邮寄的，那么就不需要单独的电子邮件客户端 213。

[0059] 一旦服务器的微处理器 304 接收到加密的会话密钥，就将其发送到模块 320，模块 320 使用逆河豚算法并结合发送器的密码，该发送器的密码根据接收器的 ID 从总线 315 上的数据库 306 得到的。然后，模块 320 的输出在模块 321 中使用用来发送该数据的 RSA 加密的私钥进一步解密。通过这些模块，能重新产生模块 310 的原来的会话密钥。

[0060] 接收到的处于压缩形式的加密的数据使用解密的会话密钥在模块 323 中进行解密，然后在模块 324 中进行解压缩。

[0061] 同模块 307 一样，解密和解压缩的数据在微处理器 304 的控制下，在模块 325 中产生 MD 散列值，模块 326 进行比较校验以将新生成的 MD 散列值和从接收器接收到的 MD 散列值进行验证以确保两者相匹配。

[0062] 假设 MD 散列值在模块 326 中验证为正确，来自模块 324 的解密的数据通过安全的链路被送回到接收器。

[0063] 图 3 是说明本发明的将数据从发送器发送到服务器的在发送器和服务器中包括的处理过程或进程的流程图。

[0064] 最初，发送器希望将特定的数据传送给具有已知接收器 ID 的特定接收器。在步骤 S1A 中，发送器和服务器通信以试图建立诸如 SSL 链接的安全通信链路。建立此链路涉及运行某些连接协议和上述的密码校验，且建立此链路能采取将万维网页显示在显示设备 105 上，在万维网页上输入适当的登录数据等等的形式。如前面提到的，建立这种通信链路和密码校验为本领域技术人员所公知，在此不作详细描述。

[0065] 响应来自发送器的联系，在步骤 S1B 中，服务器也试图通过运行某些连接协议和上述的密码校验以建立通信链路。然后，在步骤 S2B 中服务器将校验是否已经建立了有效的链路，也就是是否已经满足所有的通信协议并且已经通过了所有的密码校验。如果还没有建立起链路，或密码校验失败，服务器转到错误处理步骤 S3B。此步骤进一步包括试图建立通信链路。假设建立了有效的通信链路，该过程转到步骤 S4B，以等待接收所述接收器 ID 和被传送的数据。如果需要，此处可包括超时步骤。

[0066] 在发送器的 S2A 步骤中，进行校验以检查是否已经建立了有效的链路，也就是是否已经满足所有的通信协议并且已经通过了所有的密码校验。如果还没有建立起链路，或密码校验失败，发送器转到错误处理步骤 S3A。此步骤进一步包括试图建立通信链路。假设建立了有效的通信链路，该过程转到步骤 S4A，以发送接收器的 ID 及要传送的数据。如果需要，此处可包括超时步骤。

[0067] 在一个例子中，数据传送万维网页显示在显示设备 105 上，设备 105 需要输入接收器的 ID 和数据的附件，诸如位于数据源 108 的文件。然后将完成的数据传送页发送到服务器 300。很显然，要加密的数据可直接进入数据传送页。

[0068] 在步骤 S4B 中服务器 300 接收数据传送页的内容，之后该过程进行到步骤 S5B。在该步骤中，服务器产生对该数据唯一的 MD 散列值并将此值发送到邮件客户端 312，之后该过程进行到步骤 S6B。

[0069] 在步骤 S6B 中，该数据通过诸如压缩文件 (zipping) 压缩。然后，在步骤 S7B 中，得到来自随机数发生器 311 的随机数以生成专用于此数据传送的会话密钥。之后，在步骤

S8B 中，使用此会话密钥对数据进行加密，并将加密的数据发送到电子邮件客户端 312。

[0070] 然后过程进行到步骤 S9B，在此步骤中，使用公用 RSA（里韦斯特－沙米尔－阿德莱曼）密钥对会话密钥进行加密。之后，该过程转到步骤 S10B 以重新得到接收器的密码，之后在步骤 S11B 中，使用在步骤 S10B 重新得到的密码用河豚算法对步骤 S9B 的结果进行加密。然后将产生的加密的会话密钥发送到电子邮件客户端 312。

[0071] 在接下来的步骤 S12B 中，电子邮件客户端 312 以已知的方式，将电子邮件表示为用 HTML 传送的适当格式，诸如通过 64 位编码形式。也可以对加密的数据和加密的会话密钥使用 HTML 附加文件或插入 HTML 代码。然后发送电子邮件并且以通常的方式对电子邮件的发送进行标志，并且向发送器发送确认信息，之后该过程结束。

[0072] 显然该电子邮件包含 MD 散列值，加密的数据和优选为隐式字段的加密的会话密钥。该电子邮件优选为还包括 HTML 链接以使接收器能连接回到服务器。该链路被配置成能自动以 HTML 形式将隐式字段提交回服务器。电子邮件主题标头是由发送器选择的主题标头，并且电子邮件被编址为接收器的电子邮件的地址。

[0073] 在步骤 S5A 中，发送器接收电子邮件发送的确认信息，该过程结束。

[0074] 图 4 是说明响应从服务器接收电子邮件，在接收器和服务器中包括的处理过程或进程的流程图。

[0075] 在步骤 S101A 中，接收器 200 接收来自服务器的电子邮件，该电子邮件包含加密的数据，加密的会话密钥，和 MD 散列值，及其它。可以使用万维网邮件或使用电子邮件客户端 212 通过链接 213 下载电子邮件。在步骤 S102A 中，接收器打开电子邮件并于服务器通信以试图建立诸如 SSL 链接的安全通信链路。用与上面描述类似的方式，建立这种链路包括运行某些连接协议和类似于以上讨论的与模块 305 有关的密码校验，并采取在显示设备 105 上显示万维网页，在万维网页上输入合适的登录数据等等的形式。以前面提到的，建立这种通信链路和密码校验为本领域技术人员所公知，此处不作详细描述。

[0076] 响应来自接收器的联系，在步骤 S101B 中，服务器也试图通过运行某些连接协议和上述的密码校验来建立通信链路。在步骤 S102B 中，服务器然后检查是否已经建立了有效的链接，也就是检查是否已经满足所有的通信协议并且已经通过了所有的密码校验。如果还没有建立起链路，或密码校验失败，服务器来到错误处理步骤 S103B。这个步骤进一步包括试图建立通信链路。假如建立了有效的通信链路，该过程进行到步骤 S104B，以等待接收接收器的 ID 和包括加密的数据，加密的会话密钥和 MD 散列值的其它信息。如果需要，此处可包括超时步骤。

[0077] 在接收器的 S103A 步骤中，进行校验以检查是否已经建立了有效的链接，也就是检查是否已经满足所有的通信协议并且已经通过了所有的密码校验。如果还没有建立链路，或密码校验失败，接收器转到错误处理步骤 S104A。此步骤进一步包括试图建立通信链路。如果需要，此处可包括超时步骤。

[0078] 假如建立了有效的通信链路，该过程进行到步骤 S105A 以发送接收器 ID 及发送前面段落中提到的其它信息。后者可以以隐式 HTML 字段的形式存在于提交到服务器 300 的电子邮件中。显然，用来定时及用于排列 ID，隐藏域，密码等的发送可以不同以适应特定的情况。

[0079] 然后服务器中的过程来到步骤 S105B，以从模块 306 重新得到接收器的密码，之后

在步骤 S106B 中，使用在步骤 S105B 中重新得到的密码用河豚算法对加密的会话密钥进行解密。该过程然后转到 RSA 解密步骤 S107B，其中使用服务器的私钥对步骤 S106B 的结果进行解密。这样产生了会话密钥。

[0080] 之后，该过程来到 S108B，其中使用从步骤 S107B 中产生的解密的会话密钥对仍是压缩的数据进行解密。之后，该过程来到步骤 S109B 以对数据进行解压缩。

[0081] 在下一步骤 S110B 中，服务器产生对步骤 S109B 产生的数据唯一的 MD 散列值。之后，在步骤 S111B 中，步骤 S110B 产生的 MD 散列值相对步骤 S104B 接收到的 MD 散列值进行校验。假设该 MD 散列值是有效的，该过程进行到步骤 S113B，且现在发送器的未加密的数据通过安全链路发送到接收器。该数据的发送被标志，该过程结束。如果 MD 散列值无效，该过程分支到错误处理 S112B。这包括对错误进行标志并将错误消息发送到接收器以说明该数据已损坏或泄密。

[0082] 在步骤 S106A 中，接收器接收未加密的数据，该过程结束。

[0083] 在以上描述的发明的一个实施例中，全部的加密和解密过程都是在服务器 300 中进行的。因此，发送器和接收器不需要任何特别的软件以能安全地发送和接收数据。特别是，不需要用软件或使用硬件存储器和处理资源来进行 RSA 加密和河豚加密。此外，对密码的访问是在服务器中维护的，不需要在发送器中维护。而且，因为加密和解密是在服务器上进行的，所以发送器和接收器不需要对加密和解密进行特定的排列。

[0084] 然而，本发明还包括发送器中具有如图 2 的方框 317 中实现的功能的替代功能。也就是说，在此修改例中，随机数发生器产生的会话密钥和对数据的压缩及用此会话密钥对压缩数据的加密都是在发送器中进行的。然而，上面的安全链路是用服务器建立的，但在此情况下，只有产生的会话密钥被发送到服务器中。在与上面一样的密码校验之后，模块 S313 和模块 S314 又生成了加密的会话密钥，在此情况下，该密钥返回到发送器中。然后，加密的数据，加密的会话密钥和散列值提供给也连接到因特网的发送器的电子邮件客户端（未示出）。该电子邮件客户端如上面所述构造电子邮件，再将其发送到接收器。因此可以看出，图 3 中的从 S5B 到 S8B 的步骤是在发送器中进行的。这可以减少对服务器的处理需求。

[0085] 如图 4 所示，接收器接收电子邮件客户端的电子邮件并处理这些电子邮件。

[0086] 然而，本发明还包括接收器具有的如图 2 的方框 322 内的功能的替代功能，一旦从服务器接收到电子邮件。也就是说，在此修改例中，数据的解密，数据的解压缩，MD 散列值的产生和对其验证都是在接收器中进行的。尽管，如上面所述一样，安全链路是用服务器建立的，但在这种情况下，只有加密的会话密钥被发送到服务器。在与上面一样的密码校验之后，模块 S320 和 S321 再一次对会话密钥进行解密，在此情况下，该会话密钥返回到接收器。使用解密的会话密钥对加密的数据进行解密，并解压缩，产生的 MD 散列值相对于电子邮件中接收到的 MD 散列值进行校验其有效性。因此可以看出，图 4 中从 S108B 到 S113 的步骤在此是在接收器中进行的。这可以减少对服务器的处理需求。

[0087] 可以理解上面提到的两个修改例可同时实施。不过，对于本发明，结合接收器的密码的会话密钥的加密是在服务器中进行的。

[0088] 可以理解需要时，一组用户可被注册以接收电子邮件。例如，某公司的 IT 部门可注册所有员工。在这种情况下，当服务器的密码校验失败时，可参考该组中的其它密码。

[0089] 本发明的各种需要在发送器或接收器上安装特定软件的实施例为本领域熟练技

术人员所公知，在注册过程中，可从服务器下载并安装。

[0090] 应意识到，因为需要正确的接收器密码以用河豚算法对数据进行解密，并且因为通过验证MD散列值，可有效地校验正确的解密，所以，如果需要，可省去步骤102A中的接收器和服务器之间的链接中的密码校验。

[0091] 还应意识到，如果解密不成功，可重新安排服务器300以进一步进行校验来试图得到正确的密码，例如，可通过查询接收器的旧密码并轮流使用每一个密码来对数据进行解密。如果那些密码中有一个密码能产生正确的MD5（第五类邮件文摘）散列值，则解密成功。然而，如果没有一个密码能奏效，则接收器不是期望的接收器或在传送过程中数据已经损坏。

[0092] 如果接收器没有密码，并且还没有在服务器300上注册，服务器会产生一次性的密码，通过任何安全的方式将该密码送到接收器都是适合的，例如，通过安全邮件或通过安全链路或通过安全的电子邮件将密码送到接收器，需要用户将其密码修改成安全密码以便以后使用。

[0093] 对于本发明，检验发送器和接收器的身份以使发送器能向接收器发送数据，该接收器没有安装使接收器确信数据源的特殊软件。此外，记录加密和解密尝试的次数，这能使发送器校验接收器是否已经接收了数据并对数据进行了解密，并且能使接收器校验它们期望接收的数据是否已经发送。

[0094] 发送器和接收器设备可以采用许多形式，例如，非专属的列表包括计算机，个人数字助理或其它手持设备，膝上型电脑，移动电话。服务器优选为计算机，尽管它也可以是可替代类型的计算装置。

[0095] 可以看出，对于本发明，发送器或接受者都不知道保持在服务器上的对方的密码。因此，发送器和接收器需要的安全等级不象其它以安全方式传送数据的已知形式的那么高。

[0096] 对于本发明，服务器对在加密过程中服务器使用的接收器专用信息进行维护，诸如密码。服务器从数据存储器中得到此信息，数据存储器具有接收器ID和保密的接收器专用信息的列表。接收器专用信息可包括密码，密码短语，PIN码，散列值或用于身份验证的其它任何信息。

[0097] 用于本发明的网络可以是因特网，诸如以太网络的本地的企业内部网，电话网络，无线电网络或用于传送数据其它任何网络。优选为，当使用因特网时，在服务器和发送器之间和/或在服务器和接收器之间使用安全的SSL链接。

[0098] 通过发送器和接收器的电子邮件地址（或其它网络地址），服务器可以识别它们。尽管，它们还具有与网络地址无关的用户ID。服务器在其数据库中可具有网络地址列表，和/或具有用户ID列表，在数据库中，网络地址和/或用户ID每一个都与保密的接收器专用信息相关。

[0099] 在本发明的一个实施例中，服务器300包括对服务器唯一并仅对服务器已知的保密码。该保密码可包括在河豚加密和解密模块中。除了使用接收器专用信息外，可将保密码用于加密中。这两条信息可简单地进行级联以用于加密过程。保密密钥的使用提高了系统的安全等级。

[0100] 应意识到，服务器不需要保留会话密钥或任何发送到接收器的数据。这些密钥和

数据可存储在服务器上的非永久性存储器中，当进一步对数据和密钥进行加密时，可被重写。其具有的优点是服务器不必具有很大的存储器以存储旧的和可能冗余的数据和 / 或密钥。

[0101] 承载介质包括瞬时介质，如电，光，微波，射频，电磁，声或磁信号（如诸如因特网的 IP 网络上的 TCP IP 信号），或诸如软盘，光盘只读存储器 (CD ROM)，硬盘，或可编程存储器设备的承载介质。

[0102] 尽管此处已经根据本发明优选的实施例对其进行了描述，对本领域熟练技术人员而言，在不偏离由权利要求限定的本发明范围的前提下，对优选实施例所做的各种修改是显而易见的。本发明能应用到的领域，例如，对移动电话供应商而言，其能用安全的方式每月向移动电话用户发送账单，移动电话用户连接到服务器以获得加密的账单，银行也以类似的方式向其客户发送要付的款项细节，客户只需如上所述连接到服务器来获得这些以安全方式发送的细节。

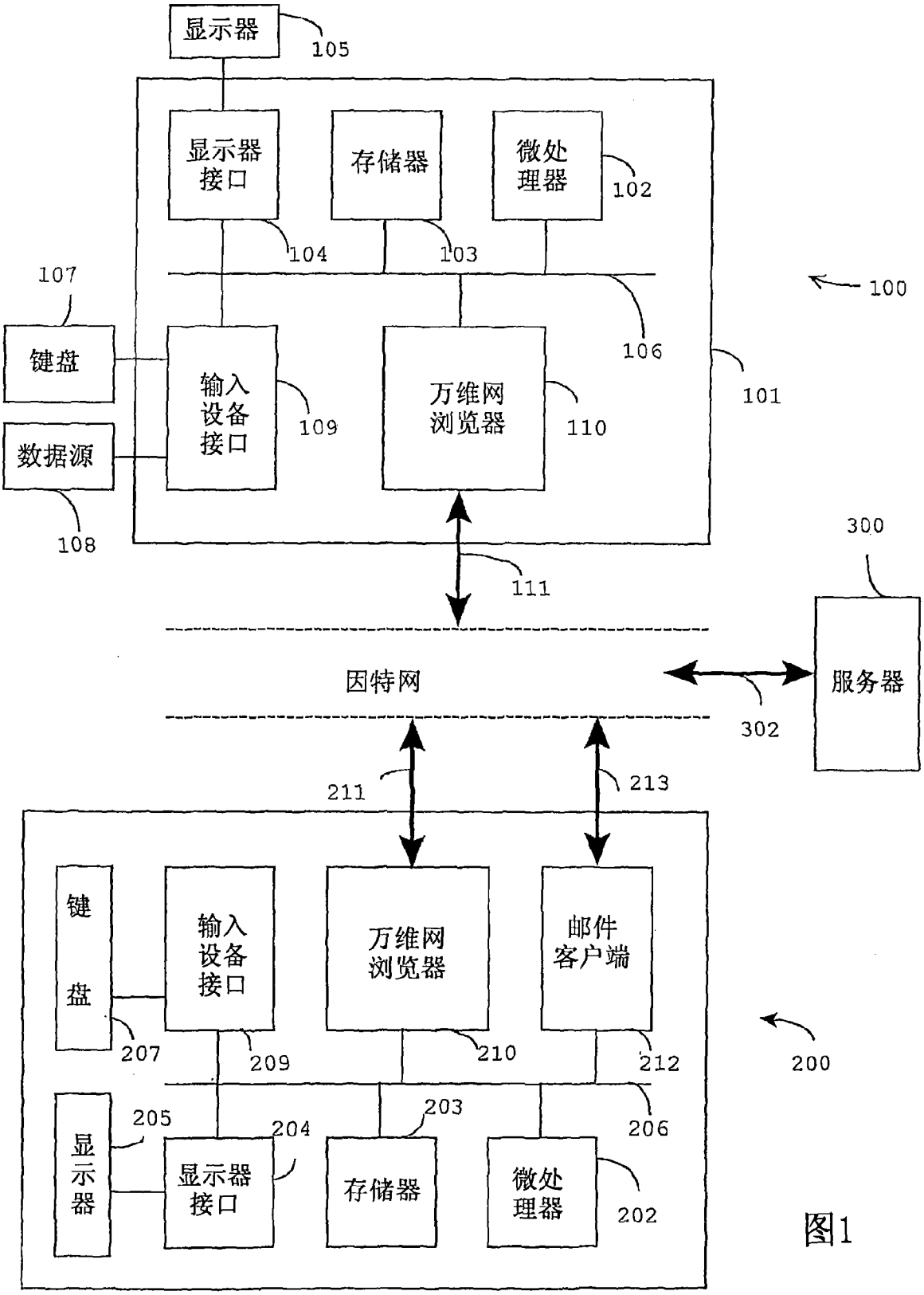

显示器
105
显示器接口
存储器
微处理器
102
104
103
107
100
键盘
输入设备接口
万维网浏览器
106
101
109
110
数据源
108
111
300
因特网
服务器
302
211
213
键盘
输入设备接口
万维网浏览器
邮件客户端
207
209
210
212
200
205
203
206
显示器
显示器接口
存储器
微处理器
204
202

图1

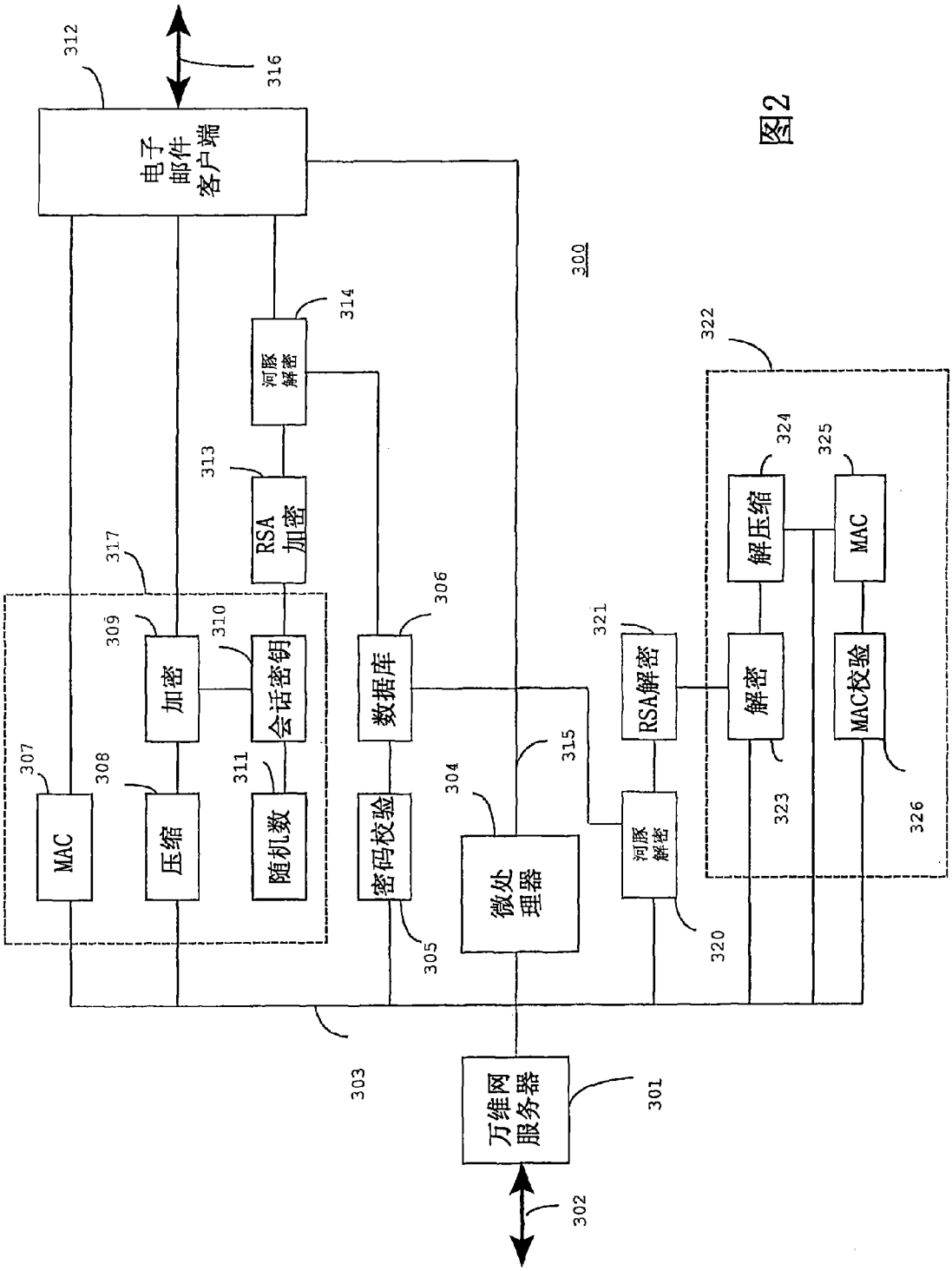

电子邮件客户端
312
316
300
河豚解密
314
RSA加密
313
317
加密
309
310
会话密钥
数据库
306
MAC
307
压缩
308
随机数
311
密码校验
304
微处理器
315
RSA解密
321
河豚解密
320
305
322
解压缩
324
MAC
325
解密
323
MAC校验
326
303
万维网服务器
301
302

图2

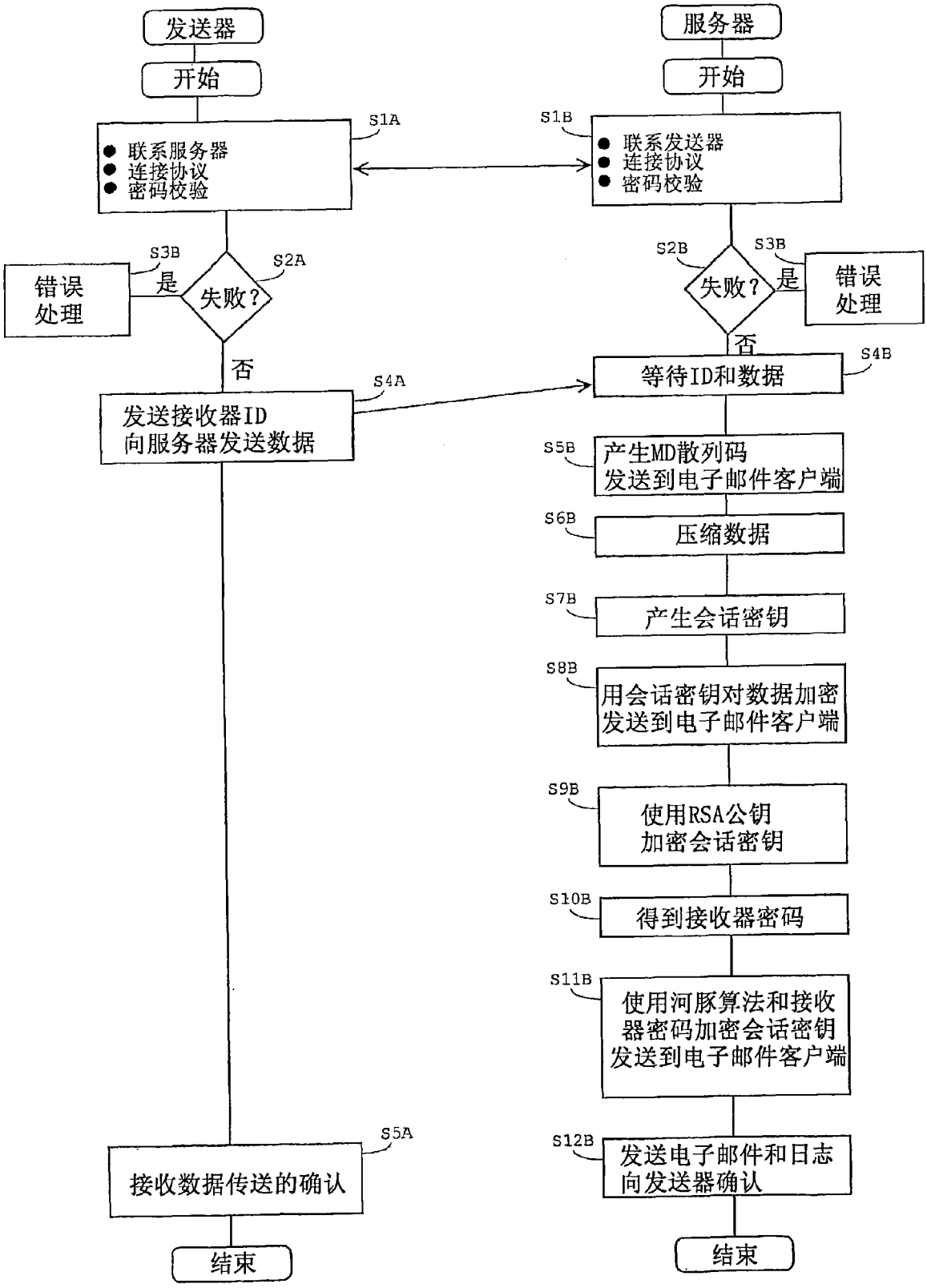

发送器
开始
S1A
联系服务器
连接协议
密码校验
S3B
是
错误处理
失败?
S2A
否
S4A
发送接收器ID
向服务器发送数据
S5A
接收数据传送的确认
结束
服务器
开始
S1B
联系发送器
连接协议
密码校验
S2B
失败?
S3B
是
错误处理
否
S4B
等待ID和数据
S5B
产生MD散列码
发送到电子邮件客户端
S6B
压缩数据
S7B
产生会话密钥
S8B
用会话密钥对数据加密
发送到电子邮件客户端
S9B
使用RSA公钥
加密会话密钥
S10B
得到接收器密码
S11B
使用河豚算法和接收
器密码加密会话密钥
发送到电子邮件客户端
S12B
发送电子邮件和日志
向发送器确认
结束

图 3

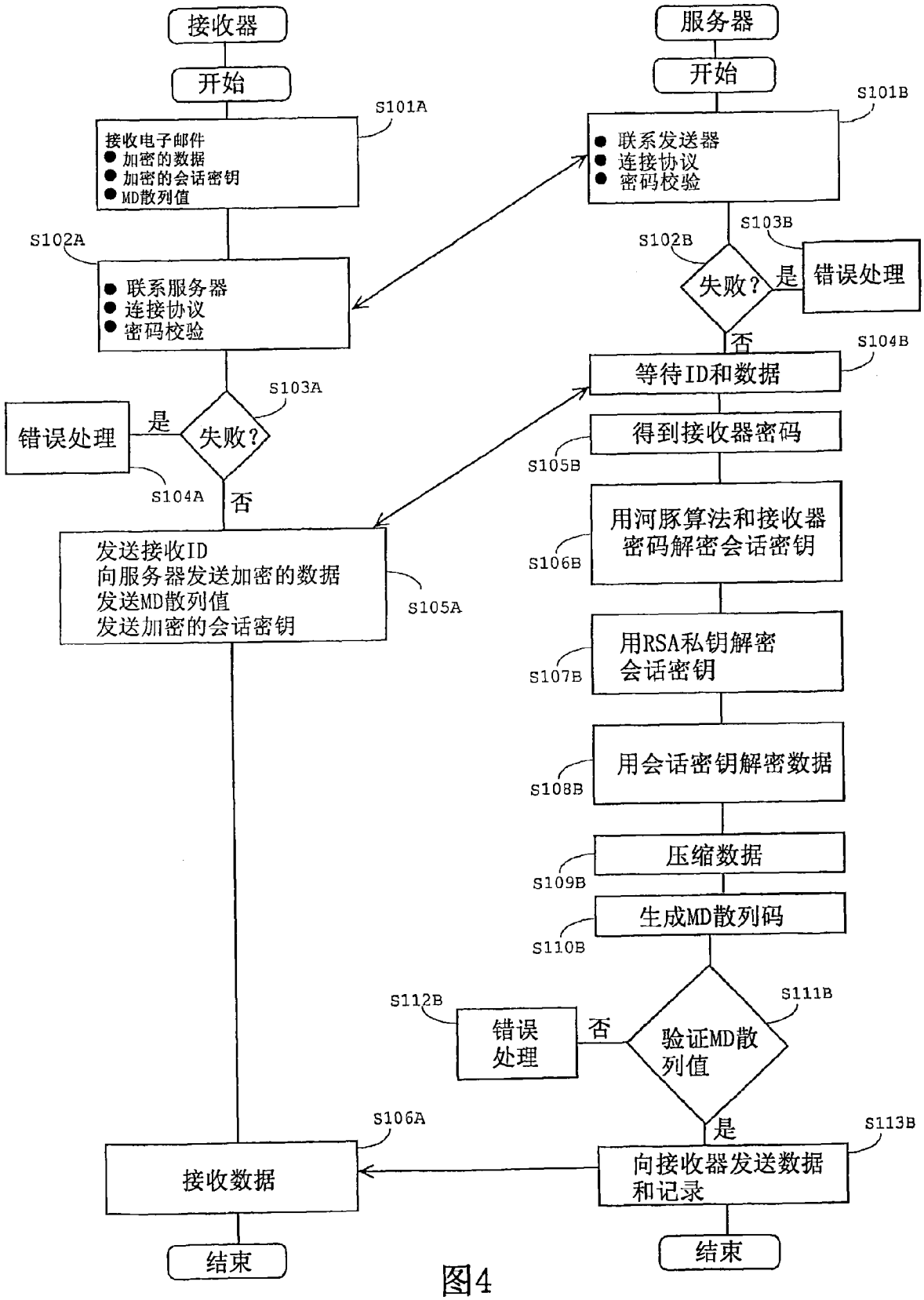

接收器
开始
S101A
接收电子邮件
● 加密的数据
● 加密的会话密钥
● MD散列值
S102A
● 联系服务器
● 连接协议
● 密码校验
S103A
失败?
是
错误处理
S104A
否
发送接收ID
向服务器发送加密的数据
发送MD散列值
发送加密的会话密钥
S105A
S106A
接收数据
结束
服务器
开始
S101B
● 联系发送器
● 连接协议
● 密码校验
S102B
失败?
是
S103B
错误处理
否
S104B
等待ID和数据
S105B
得到接收器密码
S106B
用河豚算法和接收器密码解密会话密钥
S107B
用RSA私钥解密会话密钥
S108B
用会话密钥解密数据
S109B
压缩数据
S110B
生成MD散列码
S111B
验证MD散列值
否
S112B
错误处理
是
S113B
向接收器发送数据和记录
结束

图4