电子密码生成方法、装置和设备以及电子密码认证系统

技术领域

本发明涉及信息安全领域，尤其涉及一种电子密码生成方法、装置和设备以及电子密码认证系统。

背景技术

近年来，伴随互联网以及金融信息化的快速发展，网上银行以其便利、高效等优点迅速得到用户和银行业界的普遍推崇。银行和各种大型电子商务网站为了克服基于静态口令的认证方式的安全缺陷，大多采用了动态口令令牌或动态口令卡来加强网络身份认证的安全性。

动态口令技术又称为一次性口令（One Time Password，简称 OTP）技术，其特点是用户根据服务商提供的动态口令令牌的显示数字来输入电子密码，而动态口令技术根据密码生成方式的不同，可以分为基于时间的动态口令技术和基于挑战/应答的动态口令技术。

采用基于时间的动态口令技术时，电子密码生成装置与服务器在时间上同步，并且存储有相同的密钥种子；电子密码生成装置与服务器使用该密钥种子每隔一段时间（例如，60 秒）生成一个电子密码；需要进行用户认证时，用户通过电子密码生成装置的显示屏获知当前的电子密码后，在交易终端输入该电子密码，交易终端将该电子密码以及用户名、静态密码等信息发送给服务器进行认证。

采用基于挑战/应答的动态口令技术时，电子密码生成装置与服务器存储有相同的密钥种子；需要进行用户认证时，服务器为用户生成一个挑战码，用户获得挑战码后，将挑战码输入电子密码生成装置；电子密码生成装置使用密钥种子和用户输入的挑战码生成应答码（即电子密码），用户通过电子密码生成装置的显示屏获知当前的电子密码后，在交易终端输入该电子密码，交易终端将该电子密码以及用户名、静态密码等信息发送给服务器进行认证。

上述基于动态口令技术的身份验证方式很好地克服了静态密码验证中口令信息固定不变的缺陷，但也存在如下问题：

（1）采用基于时间的动态口令技术时，电子密码并不是使用一次即失效，而是在一定时间内有效，因此当该电子密码被截获后，黑客可以使用该电子密码与服务器进行交互；例如，黑客获取到用户的账户信息时，并截获了该用户的此时间段的电子密码，即可以进

行后续的操作。即现有的采用基于时间的动态口令技术存在较大的安全隐患。

（2）采用基于挑战/应答的动态口令技术时，服务器一般是随机向用户的交易终端或手机发送挑战码的，随机挑战码与交易信息和用户信息（可以统称为用户交易信息）无关，用户无法得知是否是自身需要进行的真正的交易，也无法得知是哪一次的交易，当用户由于无法得知是否是自身需要进行的真正的交易时，而对非真正的交易进行了支付，会造成用户财产的损失，因此，服务器向用户的交易终端或手机发送随机挑战码可能会成为电子交易中一个不安全的因素。

采用基于挑战/应答的动态口令技术时，电子密码生成装置根据该挑战码生成电子密码，其中，即便挑战码采用了用户交易信息，例如账号和金额，一旦黑客获取到用户的账户信息，冒充银行给用户发送其账号和金额，并告知用户将其显示结果发送给“银行”，例如：黑客冒充银行给用户发送短信，告知其电子密码生成装置需要升级，需要用户将其发送给用户的信息输入至电子密码生成装置生成电子密码，并将电子密码反馈给黑客，通过此种方式，黑客即可以直接获得该用户的电子密码而进行后续操作，从而成为较大的安全隐患。

发明内容

本发明的目的是提供一种防止黑客进行钓鱼而导致用户损失财产的一种电子密码生成方法、装置和设备以及电子密码认证系统。

本发明的目的是通过以下技术方案实现的：

一种电子密码生成方法，包括如下步骤：通过提示信息提示用户输入挑战码，所述提示信息为包括待输入的挑战码所代表含义的信息；接收用户输入的挑战码；根据输入的所述挑战码及当前时间参数生成动态的电子密码。

此外，所述提示信息至少包括第一提示信息和第二提示信息。

此外，所述通过提示信息提示用户输入挑战码的步骤包括：通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。

此外，所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

此外，所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

此外，所述接收用户输入的挑战码的步骤包括：依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

此外，所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

此外，所述通过提示信息提示用户输入挑战码的步骤之前还包括：提示用户输入开机

密码；验证用户输入的开机密码是否正确；在验证用户输入的开机密码正确后，通过提示信息提示用户输入挑战码。

一种电子密码生成装置，该装置包括：提示单元，用于通过提示信息提示用户输入挑战码，所述提示信息为包括待输入的挑战码所代表含义的信息；接收单元，用于接收用户输入的挑战码；生成单元，用于根据输入的所述挑战码及当前时间参数生成动态的电子密码。

此外，所述提示信息至少包括第一提示信息和第二提示信息。

此外，所述提示单元具体用于：通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。

此外，所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

此外，所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

此外，所述接收单元具体用于：依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

此外，所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

此外，该装置还包括：验证单元，用于验证用户输入的开机密码是否正确，并在验证用户输入的开机密码正确后，指示提示单元通过提示信息提示用户输入挑战码。

一种电子密码生成设备，该设备包括：提示装置，用于通过提示信息提示用户输入挑战码，所述提示信息为包括待输入的挑战码所代表含义的信息；输入装置，用于输入所述挑战码；处理芯片，用于接收所述挑战码，根据所述挑战码以及当前时间参数生成电子密码。。

此外，所述提示装置包括显示装置和/或发声装置，所述显示装置用于通过文本的方式显示所述提示信息，所述发声装置用于通过语音的方式输出所述提示信息。

此外，所述输入装置包括按键和/或触摸屏。

此外，所述提示信息至少包括第一提示信息和第二提示信息。

此外，所述提示装置具体用于：通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。

此外，所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

此外，所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

此外，所述处理芯片具体用于：依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

此外，所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

此外，所述输入装置还用于输入开机密码。

此外，所述处理芯片还用于验证所述开机密码是否正确，并在验证所述开机密码正确后，指示所述提示装置通过所述提示信息提示用户输入所述挑战码。

一种电子密码认证系统，该系统包括：上述的电子密码生成设备；以及交易系统，用于根据挑战码以及当前时间参数生成交易系统端的电子密码，并在接收到电子密码生成装置端的电子密码后，将其与交易系统端的电子密码进行对比来完成认证。

一种电子密码生成方法，包括如下步骤：通过提示信息提示用户输入挑战码，所述提示信息为用户知晓其要输入的挑战码所代表含义的信息；接收用户输入的挑战码；根据输入的所述挑战码及当前时间参数生成动态的电子密码。

此外，所述提示信息至少包括第一提示信息和第二提示信息。

此外，所述通过提示信息提示用户输入挑战码的步骤包括：通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。

此外，所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

此外，所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

此外，所述接收用户输入的挑战码的步骤包括：依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

此外，所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

此外，所述通过提示信息提示用户输入挑战码的步骤之前还包括：提示用户输入开机密码；验证用户输入的开机密码是否正确；在验证用户输入的开机密码正确后，通过提示信息提示用户输入挑战码。

一种电子密码生成装置，该装置包括：提示单元，用于通过提示信息提示用户输入挑战码，所述提示信息为用户知晓其要输入的挑战码所代表含义的信息；接收单元，用于接收用户输入的挑战码；生成单元，用于根据输入的所述挑战码及当前时间参数生成动态的

电子密码。

此外，所述提示信息至少包括第一提示信息和第二提示信息。

此外，所述提示单元具体用于：通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。

此外，所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

此外，所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

此外，所述接收单元具体用于：依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

此外，所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

此外，该装置还包括：验证单元，用于验证用户输入的开机密码是否正确，并在验证用户输入的开机密码正确后，指示提示单元通过提示信息提示用户输入挑战码。

一种电子密码生成设备，该设备包括：采用上述的电子密码生成方法的处理芯片以及输入装置和提示装置；所述输入装置用于输入挑战码，所述提示装置用于提示用户知晓其要输入的挑战码所代表含义的提示信息。

一种电子密码认证系统，该系统包括：上述的电子密码生成装置以及交易系统；所述交易系统用于根据挑战码以及当前时间参数生成交易系统端的电子密码；在接收到电子密码生成装置端的电子密码后，将其与交易系统端的电子密码进行对比来完成认证。

由上述本发明提供的技术方案可以看出，本发明实施例提供的一种电子密码生成方法、装置和设备以及电子密码认证系统，由于将挑战码区分为若干部分，可以向用户提供包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

进一步，由于根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附

图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

图1为本发明实施例提供的电子密码认证系统的示意图；

图2为本发明实施例提供的电子密码认证方法的流程图；

图3为本发明实施例提供的电子密码生成方法的流程图；

图4为本发明实施例提供的电子密码生成装置的示意图；

图 5 为本发明实施例提供的电子密码生成设备的示意图。

具体实施方式

下面结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明的保护范围。

下面将结合附图对本发明实施例作进一步地详细描述。

图1示出了本发明的电子密码认证系统的示意图，参见图1，电子密码认证系统包括：交易系统以及电子密码生成装置。

交易系统可以包含：交易终端和认证服务器，交易终端和认证服务器通过局域网或者互联网或者 GSM（global system for mobile communications，全球移动通信系统）网络、3G 网络等网络与认证服务器相连。

其中，交易终端可以是银行的ATM（Automated Teller Machine，自动柜员机），也可以是个人电脑或者手机终端等设备。

认证服务器用于认证电子密码以及实现用户交易，一般为银行提供的服务器。

交易终端和认证服务器也可以合并为一个实体设备。

用户在交易终端中输入/编辑用户交易信息；交易终端将用户输入/编辑的交易报文（包括用户交易信息）逐条发送给认证服务器。其中，用户交易信息一般包括用户名、交易账号、交易金额、交易流水号等信息。

交易系统的认证服务器根据本次交易的交易报文获取本次交易的用户交易信息，将该用户交易信息作为挑战码，根据该挑战码以及当前时间参数生成交易系统端的电子密码；在接收到电子密码生成装置端的电子密码后，交易系统通过将其与交易系统端的电子密码进行对比来完成认证。其中，交易系统端的当前时间参数和电子密码生成装置的当前时间

参数在一个时间段内为相同的（例如2分钟）。

上述的挑战码可以区分为若干个部分，例如挑战码的第一信息，挑战码的第二信息，其中挑战码的每个信息为可被用户识别的代表具体含义的信息，以便用户进行确认交易是否是用户需要的真正交易。例如，挑战码的第一信息为交易账号，挑战码的第二信息为交易金额等。

电子密码生成装置可以是动态口令令牌。

电子密码生成装置用于在开机后，提示用户输入开机密码，并在验证用户输入的开机密码正确后输出包括待输入挑战码实际含义的第一提示信息，提示用户输入挑战码的第一信息（例如：交易账号），并在接收到用户输入的挑战码的第一信息后，输出包括待输入挑战码实际含义的第二提示信息，提示用户输入挑战码的第二信息（例如：交易金额），在接收到用户输入的挑战码的第二信息后，接收用户输入的确认指令，根据输入的挑战码以及当前时间参数生成电子密码生成装置端的电子密码。

当然，如果挑战码被区分为三个部分，则电子密码生成装置还可以提示用户知晓待输入挑战码实际含义的第三提示信息，例如：交易流水号、随机码等，并根据输入的挑战码和当前时间参数生成电子密码生成装置端的电子密码。

上述的第一提示信息、第二提示信息、第三提示信息可以通过显示提示或者发声提示。

通过本实施例的电子密码认证系统，由于将挑战码区分为若干部分，该系统可以向用户提供包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

本实施例根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

图2示出了本发明的电子密码认证方法的流程图，参见图2，电子密码认证方法包括：

步骤201，交易终端将用户输入/编辑的交易报文发送给认证服务器。

具体的，认证服务器中存储有各个用户的用户名、账号等信息，同时存储有该用户的电子密码生成装置的序列码、算法、当前时间参数等信息。

用户在交易终端输入/编辑交易报文时，认证服务器接收交易报文，获取交易报文中的用户交易信息。

步骤202，认证服务器根据用户交易信息生成挑战码，并根据该挑战码以及当前时间参数生成交易系统端的电子密码。

具体的，认证服务器可以根据与输入至电子密码生成装置中的挑战码一致的挑战码结合与电子密码生成装置中的当前时间参数一致的当前时间参数生成交易系统端的电子密码。

步骤203，电子密码生成装置校验开机密码。

具体的，电子密码生成装置在开机时，提示用户输入开机密码，在接收到用户输入的开机密码后，校验该开机密码是否正确，校验正确则执行后续操作，否则提示输入错误，在输入预定次数（例如3次）均错误后，锁定该电子密码生成装置，或者一旦校验开机密码输入错误，直接锁定该电子密码生成装置。

步骤204，电子密码生成装置提示用户输入挑战码的第一信息。

具体的，电子密码生成装置在校验开机密码正确后，输出包括待输入挑战码实际含义的第一提示信息，提示用户输入挑战码的第一信息。

例如：开机密码验证正确后，电子密码生成装置输出包括待输入挑战码实际含义的第一提示信息，例如“请输入交易账号”，提示用户输入交易账号，用户将交易终端上显示的用户交易信息中的交易账号输入至电子密码生成装置。也就是用户输入的交易账号为挑战码的第一信息。

步骤205，电子密码生成装置提示用户输入挑战码的第二信息。

具体的，电子密码生成装置在接收到用户输入的挑战码的第一信息后，根据用户的确认指令，输出包括待输入挑战码实际含义的第二提示信息，提示用户输入挑战码的第二信息；或者判断用户输入的挑战码的第一信息的位数是否为预设位数，如果是则输出包括待输入挑战码实际含义的第二提示信息，提示用户输入挑战码的第二信息。

例如：在电子密码生成装置提示用户输入交易账号，用户将交易终端上显示的用户交易信息中的交易账号输入至电子密码生成装置后，电子密码生成装置输出包括待输入挑战码实际含义的第二提示信息，例如“请输入交易金额”，提示用户输入交易金额，用户将交易终端上显示的用户交易信息中的交易金额输入至电子密码生成装置。也就是用户输入的交易金额为挑战码的第二信息。

当然，在电子密码生成装置在接收到用户输入的挑战码的第二信息后，还可以输出包括待输入挑战码实际含义的第三提示信息，提示用户输入挑战码的第三信息，以进一步提高安全性。

上述的第一提示信息、第二提示信息、第三提示信息可以通过显示提示或者发声提示。

步骤206，电子密码生成装置接收用户的确认指令，根据输入的挑战码和当前时间参数生成电子密码。

具体的，在用户输入完挑战码的第一信息和挑战码的第二信息后，接收用户的确认指令，表明挑战码全部输入完毕，根据输入的挑战码（该挑战码与交易系统显示的挑战码一致）和当前时间参数（该当前时间参数与认证服务器的当前时间参数一致）根据预设的算法生成电子密码。

其中，生成电子密码的过程为现有技术，在此不再赘述。

步骤207，交易系统接收用户输入的电子密码生成装置端的电子密码，并与交易系统端的电子密码对比进行认证。

具体的，交易终端接收用户输入的电子密码生成装置端的电子密码，并将该电子密码发送给认证服务器，认证服务器接收该电子密码，并与之前生成的交易系统端的电子密码进行对比，对比一致则进行后续处理，否则反馈提示信息至交易终端，交易终端提示用户输入错误，在输入预定次数（例如3次）均错误后，锁定该电子密码生成装置，或者一旦交易系统端的电子密码输入错误，直接关闭与该电子密码生成装置对应的所有功能。

进一步，交易终端可以将接收到的电子密码生成装置端的电子密码根据预设的加密算法加密后发送给认证服务器，认证服务器对加密后的电子密码通过预设的解密算法进行解密得到电子密码生成装置端的电子密码，并与之前生成的交易系统端的电子密码进行对比，对比一致则进行后续处理。通过加密电子密码的方式，防止该电子密码在传输过程中被截取，提高了安全性。

当然，本实施例的步骤204和步骤205可以同时进行，即电子密码生成装置同时提示用户输入挑战码的第一信息和提示用户输入挑战码的第二信息。在用户输入全部挑战码后，接收用户的确认指令，根据输入的挑战码和当前时间参数生成电子密码。

通过本实施例的电子密码认证方法，由于将挑战码区分为若干部分，并向用户提供包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

本实施例根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

图3示出了本发明电子密码生成方法的流程图，参见图3，电子密码生成方法包括如下步骤：

步骤301，通过提示信息提示用户输入挑战码，提示信息为包括待输入的挑战码所代表含义的信息。

具体的，提示信息至少包括第一提示信息和第二提示信息。其中，通过第一提示信息提示用户输入挑战码的第一信息；通过第二提示信息提示用户输入挑战码的第二信息。第一提示信息可以为提示用户输入交易账号的信息，第二提示信息可以为提示用户输入交易金额的信息。

当然，在步骤301之前，还可以提示用户输入开机密码，并验证用户输入的开机密码是否正确，在验证用户输入的开机密码正确后，再通过提示信息提示用户输入挑战码。

步骤302，接收用户输入的挑战码。

具体的，挑战码至少包括挑战码的第一信息和挑战码的第二信息。

依次接收用户输入的挑战码的第一信息和挑战码的第二信息，直至全部挑战码接收完毕。其中，挑战码的第一信息可以为交易账号，挑战码的第二信息可以为交易金额。

步骤303，根据输入的挑战码及当前时间参数生成动态的电子密码。

通过本实施例的电子密码生成方法，由于将挑战码区分为若干部分，并向用户提供包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

本实施例根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

图4示出了本发明电子密码生成装置的示意图，参见图4，电子密码生成装置可以包括：输入单元，接收单元，验证单元，提示单元，生成单元。

输入单元，用于为用户提供输入的按键或者触摸屏等。

接收单元，用于接收用户输入的开机密码、挑战码的第一信息、挑战码的第二信息、确认指令或者取消指令等控制指令信息。

验证单元用于验证接收单元接收到的用户输入的开机密码是否正确。

提示单元用于提示用户输入开机密码，并在验证单元验证用户输入的开机密码正确后向用户提供包括待输入挑战码实际含义的第一提示信息，提示用户输入挑战码的第一信息，并在接收单元接收到用户输入的挑战码的第一信息后，向用户提供包括输入挑战码实际含义的第二提示信息，提示用户输入挑战码的第二信息。其中，第一提示信息和第二提示信息为显示提示（通过文本提示）或者发声提示（通过语音的方式提示）。

生成单元，在接收单元接收到用户输入的确认指令后，根据输入的挑战码以及当前时间参数生成电子密码生成装置端的电子密码。

当然，如果挑战码被区分为三个部分，提示单元还用于在接收单元接收到用户输入的挑战码的第二信息后，向用户提供包括待输入挑战码实际含义的第三提示信息，提示用户输入挑战码的第三信息。第三提示信息也可以通过显示提示或者发声提示。

通过本实施例的电子密码生成装置，由于将挑战码区分为若干部分，该生成装置可以向用户提供包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

本实施例根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

图5示出了本发明电子密码生成设备的示意图，参见图5，电子密码生成设备包括：提示装置，输入装置，处理芯片，电源等。

电源为电子密码生成设备的各个模块（如提示装置、输入装置、处理芯片等）进行供电。

输入装置为按键或者触摸屏，用于为用户提供输入开机密码、挑战码的第一信息、挑战码的第二信息、确认指令或者取消指令等控制指令信息的介质。

提示装置，包括显示装置或者发声装置，用于提示用户输入开机密码，并在处理芯片验证用户输入的开机密码正确后输出包括待输入挑战码实际含义的第一提示信息，提示用户输入挑战码的第一信息，并在处理芯片接收到用户输入的挑战码的第一信息后，输出包括待输入挑战码实际含义的第二提示信息，提示用户输入挑战码的第二信息。其中，第一提示信息和第二提示信息为通过显示装置显示提示或者通过发声装置发声提示。

处理芯片用于验证用户输入的开机密码是否正确，控制显示装置或者发声装置提示提

示信息，以及根据输入的挑战码以及当前时间参数生成电子密码。

当然，如果挑战码被区分为三个部分，显示装置或者发声装置还用于在处理芯片接收到用户输入的挑战码的第二信息后，输出包括待待输入挑战码实际含义的第三提示信息，提示用户输入挑战码的第三信息。第三提示信息业可以通过显示装置显示提示或者通过发声装置发声提示。

通过本实施例的电子密码生成设备，将挑战码区分为若干部分，该生成设备可以输出包括待输入挑战码实际含义的提示信息，用户根据提示信息依次输入挑战码的每个部分，从而可以根据提示信息以及输入的挑战码来确认此次交易是否是用户需要的真正交易，从一定程度上防止了黑客进行钓鱼的行为，保证了用户财产的安全。

本实施例根据挑战码和当前时间参数生成动态的电子密码，可以保证即便是相同的挑战码（例如给同一账户汇款相同金额），也可以生成不同的电子密码，进一步保证了电子密码的安全性。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明披露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求书的保护范围为准。

权利要求书

1、一种电子密码生成方法，其特征在于，包括如下步骤：

通过提示信息提示用户输入挑战码，所述提示信息为包括待输入的挑战码所代表含义的信息；

接收用户输入的挑战码；

根据输入的所述挑战码及当前时间参数生成动态的电子密码。

2、根据权利要求1所述的方法，其特征在于，

所述提示信息至少包括第一提示信息和第二提示信息。

3、根据权利要求2所述的方法，其特征在于，所述通过提示信息提示用户输入挑战码的步骤包括：

通过第一提示信息提示用户输入挑战码的第一信息；

通过第二提示信息提示用户输入挑战码的第二信息。

4、根据权利要求2或3所述的方法，其特征在于，

所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

5、根据权利要求1所述的方法，其特征在于，

所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

6、根据权利要求5所述的方法，其特征在于，所述接收用户输入的挑战码的步骤包括：

依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

7、根据权利要求5或6所述的方法，其特征在于，

所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

8、根据权利要求1-7任一项所述的方法，其特征在于，所述通过提示信息提示用户输入挑战码的步骤之前还包括：

提示用户输入开机密码；

验证用户输入的开机密码是否正确；

在验证用户输入的开机密码正确后，通过提示信息提示用户输入挑战码。

9、一种电子密码生成设备，其特征在于，包括：

提示装置，用于通过提示信息提示用户输入挑战码，所述提示信息为包括待输入的挑战码所代表含义的信息；

输入装置，用于输入所述挑战码；

处理芯片，用于接收所述挑战码，根据所述挑战码以及当前时间参数生成电子密码。

10、根据权利要求9所述的设备，其特征在于，所述提示装置包括显示装置和/或发声装置，所述显示装置用于通过文本的方式显示所述提示信息，所述发声装置用于通过语音的方式输出所述提示信息。

11、根据权利要求9所述的设备，其特征在于，所述输入装置包括按键和/或触摸屏。

12、根据权利要求9所述的设备，其特征在于，

所述提示信息至少包括第一提示信息和第二提示信息。

13、根据权利要求9至12中任一项所述的设备，其特征在于，所述提示装置具体用于：

通过第一提示信息提示用户输入挑战码的第一信息；

通过第二提示信息提示用户输入挑战码的第二信息。

14、根据权利要求9至13中任一项所述的设备，其特征在于，

所述第一提示信息为提示用户输入交易账号的信息，所述第二提示信息为提示用户输入交易金额的信息。

15、根据权利要求9所述的设备，其特征在于，

所述挑战码至少包括挑战码的第一信息和挑战码的第二信息。

16、根据权利要求15所述的设备，其特征在于，所述处理芯片具体用于：

依次接收用户输入的挑战码的第一信息和挑战码的第二信息。

17、根据权利要求15或16所述的装置，其特征在于，

所述挑战码的第一信息为交易账号，所述挑战码的第二信息为交易金额。

18、根据权利要求9所述的装置，其特征在于，所述输入装置还用于输入开机密码。

19、根据权利要求18所述的设备，其特征在于，所述处理芯片还用于验证所述开机密码是否正确，并在验证所述开机密码正确后，指示所述提示装置通过所述提示信息提示用户输入所述挑战码。

20、一种电子密码认证系统，其特征在于，该系统包括：

如权利要求9-19中任一项所述的电子密码生成设备；以及

交易系统，用于根据挑战码以及当前时间参数生成交易系统端的电子密码，并在接收到所述电子密码生成设备端的电子密码后，将所述电子密码生成设备端的电子密码与交易系统端的电子密码进行对比来完成认证。