(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 102752110 B
(45)授权公告日 2015.04.15

(21)申请号 201110098297.6

(22)申请日 2011.04.19

(73)专利权人 中国银行股份有限公司
地址 100818 北京市西城区复兴门内大街1号

(72)发明人 王炯 王海炜 潘定 庄向友 林启琴 方晨 陈丹霞

(74)专利代理机构 北京金信知识产权代理有限公司 11225
代理人 黄威 孙丽梅

(51)Int.Cl.
*H04L 9/32*(2006.01)

(56)对比文件
CN 101577917 A,2009.11.11,
CN 101777158 A,2010.07.14,
CN 101777983 A,2010.07.14,
US 2006/0039558 A1,2006.02.23,
CN 1869997 A,2006.11.29,

审查员 郭婧

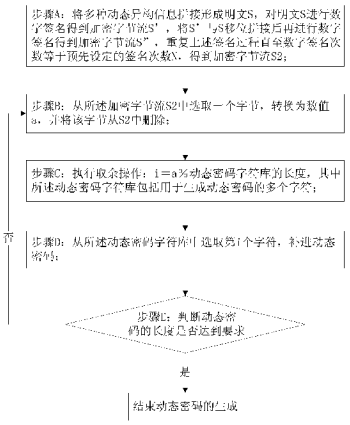
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种动态密码生成方法及系统

(57)摘要

本发明公开了一种动态密码生成方法及系统，所述方法包括：将多种动态异构信息拼接形成明文S，对明文S进行N次数字签名得到加密字节流S2；从S2中选取一个字节，转换为数值a；执行取余操作：i＝a%动态密码字符库的长度；从动态密码字符库中选取第i个字符，补进动态密码；重复上述动态密码生成过程，直至动态密码长度达到要求；所述系统包括明文拼接模块、签名模块、转换模块、动态密码字符库、取余模块、密码拼接模块和判别模块。本发明提供的动态密码生成方集中了随机数算法和数字签名算法的优点，使得同样的交易、同样的操作员不同时间来操作，所获得动态密码绝不一样；且动态密码仅在使用时产生，重复率极低，具备较高的安全性。




CN 102752110 B

1. 一种动态密码生成方法，其特征在于，包括：

步骤 A：将多种动态异构信息拼接形成明文 S，对明文 S 进行数字签名得到加密字节流 S'，将 S' 与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；

步骤 B：从所述加密字节流 S2 中选取一个字节，转换为数值 a，并将该字节从 S2 中删除；

步骤 C：执行取余操作：i = a%动态密码字符库的长度，其中所述动态密码字符库包括用于生成动态密码的多个字符；

步骤 D：从所述动态密码字符库中选取第 i 个字符，补进动态密码；

步骤 E：判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则重复步骤 B 至步骤 E 的过程。

2. 根据权利要求 1 所述的动态密码生成方法，其特征在于，所述步骤 A 中，所述多种动态异构信息包括交易信息、操作员信息、时间、随机数、预留文本库中的随机字段和高斯随机数，其中，所述预留文本库中存储公开网页，所述预留文本库中的随机字段的长度的最小值为 10 位。

3. 根据权利要求 1 所述的动态密码生成方法，其特征在于，所述步骤 C 和步骤 D 中，所述动态密码字符库中的字符为数字、英文字母和标点符号。

4. 根据权利要求 3 所述的动态密码生成方法，其特征在于，所述步骤 C 和步骤 D 中，所述动态密码字符库不包括数字 0 和字母 o，数字 1 和字母 l，数字 2 和字母 z。

5. 根据权利要求 1 所述的动态密码生成方法，其特征在于，所述步骤 C 和步骤 D 中，所述动态密码字符库中的字符的排列顺序定期进行调整。

6. 根据权利要求 1 所述的动态密码生成方法，其特征在于，所述步骤 E 中，所述动态密码的长度要求的范围是 6-10 位。

7. 根据权利要求 1 所述的动态密码生成方法，其特征在于，所述步骤 A 中，所述数字签名的方法为 MD5 或 SHA。

8. 一种动态密码生成系统，其特征在于，包括明文拼接模块、签名模块、转换模块、动态密码字符库、取余模块、密码拼接模块和判别模块，其中：

所述明文拼接模块，用于将多种动态异构信息拼接形成明文 S；

所述签名模块，用于对明文 S 进行数字签名得到加密字节流 S'，将 S' 与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；

所述转换模块，用于从所述加密字节流 S2 中选取一个字节，转换为数值 a，并将该字节从 S2 中删除；

所述动态密码字符库，包括用于生成动态密码的多个字符；

所述取余模块，用于执行取余操作：i = a%动态密码字符库的长度；

所述密码拼接模块，用于从所述动态密码字符库中选取第 i 个字符，补进动态密码；

所述判别模块，用于判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则继续动态密码的生成。

9. 根据权利要求 8 所述的动态密码生成系统，其特征在于，所述多种动态异构信息包

括交易信息、操作员信息、时间、随机数、预留文本库中的随机字段和高斯随机数，其中，所述预留文本库中存储公开网页，所述预留文本库中的随机字段的长度的最小值为 10 位。

10. 根据权利要求 8 所述的动态密码生成系统，其特征在于，所述签名模块是 MD5 加密系统或 SHA 加密系统。

# 一种动态密码生成方法及系统

## 技术领域

[0001] 本发明属于信息安全技术领域，特别涉及一种动态密码生成方法及系统。

## 背景技术

[0002] 随着互联网应用服务的普及，用户在网络上进行的交易越来越多。由于互联网的开放性、不可靠性及对等性，使得信息安全成为一个关键问题。尤其对基于互联网的网上银行服务来说，信息安全是最基础、最关键、最需要关注的部分。

[0003] 用户在使用网上银行的高风险业务时，如转账业务、支付业务等，必须输入正确的密码，银行才会为用户提供服务。通常，用户输入的密码是其账户的固有密码，因为用户输入的固有密码必须通过互联网传送给业务中心的服务器，所以输入固有密码会降低交易的安全性，非法攻击者很容易通过网络攻击等方式盗取用户的固有密码。

[0004] 为了防止因用户的固有密码被盗而带来的危险，目前增加了动态密码进行验证的方式来进行交易，即用户不仅需要输入固有密码，还需要输入每次交易均会变化的动态密码，如现有技术的动态口令牌就提供了这样一种动态密码。

[0005] 现有技术的动态口令牌主要使用 N 位种子和时间生成密码，黑客获知 N 位种子和动态口令的生成算法，就能破解密码；此外动态口令牌生成密码所采用的密码库中的字符主要为数字，使得生成的动态密码的值域范围很小，降低了破解的难度。

## 发明内容

[0006] 为了解决现有技术的上述问题，本发明的目的是提供一种结合了随机数算法的难以破解的动态密码生成方法及系统。

[0007] 为了实现上述目的，本发明提供了一种动态密码生成方法，其特征在于，包括：

[0008] 步骤 A：将多种动态异构信息拼接形成明文 S，对明文 S 进行数字签名得到加密字节流 S'，将 S'与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；

[0009] 步骤 B：从所述加密字节流 S2 中选取一个字节，转换为数值 a，并将该字节从 S2 中删除；

[0010] 步骤 C：执行取余操作：i = a%动态密码字符库的长度，其中所述动态密码字符库包括用于生成动态密码的多个字符；

[0011] 步骤 D：从所述动态密码字符库中选取第 i 个字符，补进动态密码；

[0012] 步骤 E：判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则重复步骤 B 至步骤 E 的过程。

[0013] 作为优选，所述步骤 A 中，所述多种动态异构信息包括交易信息、操作员信息、时间、随机数、预留文本库中的随机字段和高斯随机数，其中，所述预留文本库中存储公开网页，所述预留文本库中的随机字段的长度的最小值为 10 位。

[0014] 作为优选，所述步骤 C 和步骤 D 中，所述动态密码字符库中的字符为数字、英文字

母和标点符号。

[0015] 作为进一步地优选，所述步骤 C 和步骤 D 中，所述动态密码字符库不包括数字 0 和字母 o，数字 1 和字母 l，数字 2 和字母 z。

[0016] 作为优选，所述步骤 C 和步骤 D 中，所述动态密码字符库中的字符的排列顺序定期进行调整。

[0017] 作为优选，所述步骤 E 中，所述动态密码的长度要求的范围是 6-10 位。

[0018] 作为优选，所述步骤 A 中，所述数字签名的方法为 MD5 或 SHA。

[0019] 本发明同时还提供了一种动态密码生成系统，包括明文拼接模块、签名模块、转换模块、动态密码字符库、取余模块、密码拼接模块和判别模块，其中：

[0020] 所述明文拼接模块，用于将多种动态异构信息拼接形成明文 S；

[0021] 所述签名模块，用于对明文 S 进行数字签名得到加密字节流 S'，将 S' 与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；

[0022] 所述转换模块，用于从所述加密字节流 S2 中选取一个字节，转换为数值 a，并将该字节从 S2 中删除；

[0023] 所述动态密码字符库，包括用于生成动态密码的多个字符；

[0024] 所述取余模块，用于执行取余操作：i ＝ a%动态密码字符库的长度；

[0025] 所述密码拼接模块，用于从所述动态密码字符库中选取第 i 个字符，补进动态密码；

[0026] 所述判别模块，用于判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则继续动态密码的生成。

[0027] 作为优选，所述多种动态异构信息包括交易信息、操作员信息、时间、随机数、预留文本库中的随机字段和高斯随机数，其中，所述预留文本库中存储公开网页，所述预留文本库中的随机字段的长度的最小值为 10 位。

[0028] 作为优选，所述签名模块是 MD5 加密系统或 SHA 加密系统。

[0029] 与现有技术相比，本发明具有以下有益效果：

[0030] (1) 动态密码字符库包括数字、英文字母和标点符号，较动态口令牌大为扩展，使得动态密码的值域范围扩大，动态密码难于理解，增加了破解的难度；

[0031] (2) 结合了交易独特性和操作员身份唯一性，集中了随机数算法和数字签名算法的优点，使得同样的交易、同样的操作员不同时间来操作，所获得动态密码绝不一样；且动态密码仅在使用时产生，一次有效，重复率极低，具备较高的安全性；

[0032] (3) 动态密码生成过程中使用了数字签名，具备较高的加密强度、计算复杂性和不可倒推性，因此很难从密码本身推导出明文，很难掌握动态密码的生成规律，密码生成算法在保密性上不逊色于动态口令牌；

[0033] (4) 签名所使用的明文中加入了随机数，即使黑客获知签名所用的明文和签名算法，还需同步随机数发生器才有可能破解密码，破解难度大为增加。

## 附图说明

[0034] 图 1 为本发明的动态密码生成方法的流程示意图。

[0035] 图 2 为本发明的动态密码生成系统的结构示意图。

## 具体实施方式

[0036] 下面结合附图对本发明的实施例进行详细说明。

[0037] 图 1 为本发明的动态密码生成方法的流程示意图。如图 1 所示，本发明提供的动态密码生成方法包括：

[0038] 步骤 A：将多种动态异构信息拼接形成明文 S，对明文 S 进行数字签名得到加密字节流 S'，将 S'与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；

[0039] 步骤 B：从所述加密字节流 S2 中选取一个字节，转换为数值 a，并将该字节从 S2 中删除；

[0040] 步骤 C：执行取余操作：i = a%动态密码字符库的长度，其中所述动态密码字符库包括用于生成动态密码的多个字符；

[0041] 步骤 D：从所述动态密码字符库中选取第 i 个字符，补进动态密码；

[0042] 步骤 E：判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则重复步骤 B 至步骤 E 的过程。

[0043] 所述步骤 A 中，所述明文 S 可以通过以下方法拼接形成：

[0044] 1、从预留文本库中随机截取三个不同的字符串 R1、R2 和 R3；

[0045] 所述预留文本库为自建字符串库，其中存储着大量公开网页，截取的字符串 R1、R2 和 R3 的长度最小值为 10 位；

[0046] 2、将操作员信息、R1、时间值、R2、随机数、交易信息、R3 与高斯随机数组合拼接在一起，形成明文 S。

[0047] 由于签名所使用的明文中加入了随机数，即使黑客获知签名所用的明文和签名算法，还需同步随机数发生器才有可能破解密码，破解难度大为增加。

[0048] 所述步骤 A 中，所采用的数字签名的算法不唯一，签名的主要目的是以字符串明文为输入，产生一个看似与明文毫无关系并极为混乱的加密字节流，可供选择的数字签名算法有 MD5(Message Digest Algorithm MD5，消息摘要算法第五版)、SHA(Secure Hash Algorithm，安全散列算法) 等。

[0049] 所述步骤 B 中，所述数值 a 是指选取的字节在计算机中对应的数值。

[0050] 所述步骤 C 和步骤 D 中，所述动态密码字符库中的字符有数字、英文字母和标点符号，并且删去容易混淆的数字和英文字母，如数字 0 和字母 o，数字 1 和字母 l，数字 2 和字母 z 等，以免用户在使用动态密码时弄错；动态密码字符库中的字符举例如下：c，x，～，%，7，/，8，v，！，e，6，a，h，}，n，：，；，#，，9，g，*，<，f，p，>，@，5，(，)，-，＝，w，i，u，+，\，d，q，&，[，k，r，]，{ 等。

[0051] 由于所述动态密码字符库包括数字、英文字母和标点符号，较动态口令牌大为扩展，使得动态密码的值域范围扩大，动态密码难于理解，增加口了破解的难度。

[0052] 因为动态密码的生成依赖于动态密码字符库中的字符的排列顺序，所以，为了确保本发明的动态密码生成方法的安全，需要定期对动态密码字符库中字符的排列顺序进行调整，如一年调整一次，以防范破解者进行共谋破解。

[0053] 所述步骤 E 中，生成动态密码时，动态密码的初始长度设为 0，生成的所述动态密码的长度要求的范围是 6-10 位，该长度范围内的动态密码不但能保证安全性，而且使用起来比较方便。

[0054] 本发明提供的动态密码生成方法结合了交易独特性和操作员身份唯一性，集中了随机数算法和数字签名算法的优点，使得同样的交易、同样的操作员不同时间来操作，所获得动态密码绝不一样，增加了破解的难度。

[0055] 由于动态密码生成过程中使用了数字签名，具备较高的加密强度、计算复杂性和不可倒推性，因此很难从密码本身推导出明文，很难掌握动态密码的生成规律，密码生成算法在保密性上不逊色于动态口令牌。

[0056] 图 2 为本发明的动态密码生成系统的结构示意图。如图 2 所示，本发明提供的动态密码生成系统包括明文拼接模块、签名模块、转换模块、动态密码字符库、取余模块、密码拼接模块和判别模块，其中：

[0057] 所述明文拼接模块，用于将多种动态异构信息拼接形成明文 S；所述多种动态异构信息包括交易信息、操作员信息、时间、随机数、预留文本库中的随机字段和高斯随机数，其中，所述预留文本库中存储公开网页，所述预留文本库中的随机字段的长度的最小值为 10 位；

[0058] 所述签名模块，用于对明文 S 进行数字签名得到加密字节流 S'，将 S' 与 S 移位拼接后再进行数字签名得到加密字节流 S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数 N，得到加密字节流 S2；所述签名模块采用的数字签名的算法不唯一，签名的主要目的是以字符串明文为输入，产生一个看似与明文毫无关系并极为混乱的加密字节流，可供选择的签名系统有 MD5 加密系统 (Message Digest Algorithm MD5，消息摘要算法第五版)、SHA 加密系统 (Secure Hash Algorithm，安全散列算法) 等；

[0059] 所述转换模块，用于从所述加密字节流 S2 中选取一个字节，转换为该字节在计算机中的数值 a，并将该字节从 S2 中删除；

[0060] 所述动态密码字符库，包括用于生成动态密码的多个字符，如数字、英文字母和标点符号，并且为了避免用户在使用动态密码时弄错，删去容易混淆的数字和英文字母，如数字 0 和字母 o，数字 1 和字母 l，数字 2 和字母 z 等；动态密码字符库中的字符举例如下：c，x，～，％，7，/，8，v，！，e，6，a，h，}，n，：，；，#，，9，g，*，<，f，p，>，@，5，(，)，-，＝，w，i，u，+，\，d，q，&，[，k，r，]，{ 等；并且由于动态密码的生成依赖于动态密码字符库中的字符的排列顺序，所以，为了确保本发明的动态密码生成系统的安全性，需要定期对动态密码字符库中字符的排列顺序进行调整，如一年调整一次，以防范破解者进行共谋破解；

[0061] 所述取余模块，用于执行取余操作：i ＝ a％动态密码字符库的长度，得到数值 a 对动态密码字符库的长度取余的结果 i；

[0062] 所述密码拼接模块，用于从所述动态密码字符库中选取第 i 个字符，补进动态密码；

[0063] 所述判别模块，用于判断动态密码的长度是否达到要求，如果达到要求，则结束动态密码的生成，如果未达到要求，则继续动态密码的生成。

[0064] 以上实施例仅为本发明的示例性实施例，不用于限制本发明，本发明的保护范围由权利要求书限定。本领域技术人员可以在本发明的实质和保护范围内，对本发明做出各

种修改或等同替换，这种修改或等同替换也应视为落在本发明的保护范围内。

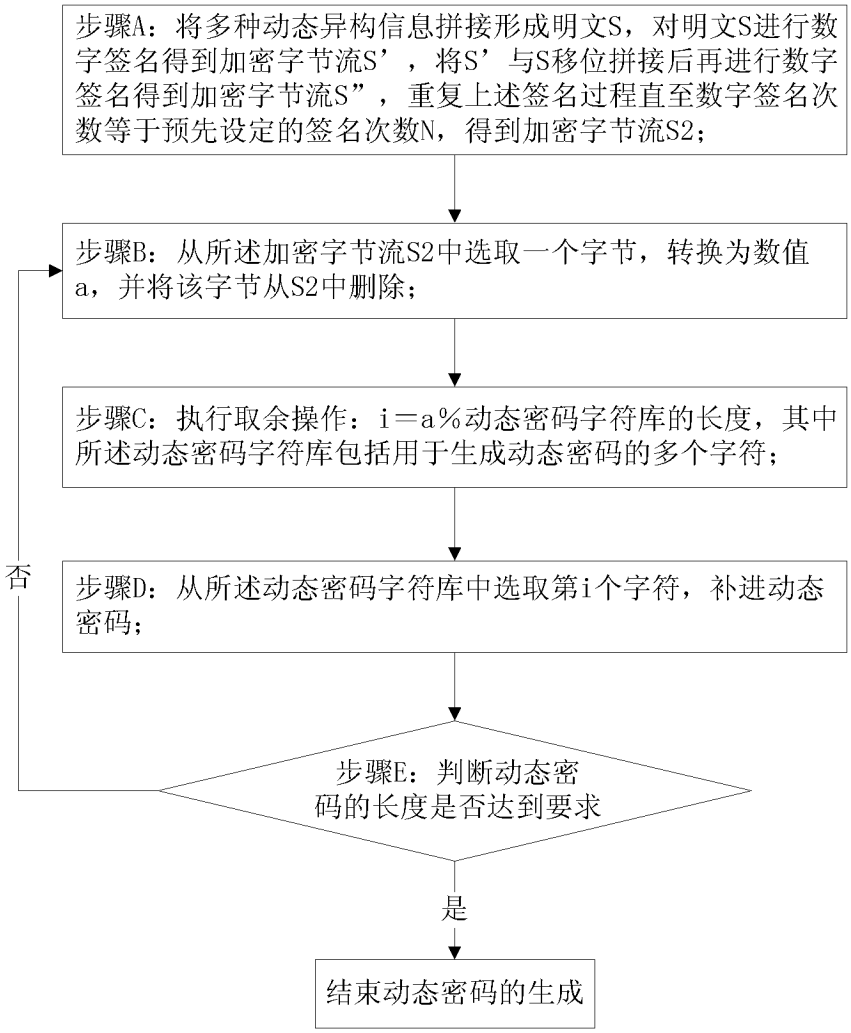

步骤A：将多种动态异构信息拼接形成明文S，对明文S进行数字签名得到加密字节流S'，将S'与S移位拼接后再进行数字签名得到加密字节流S"，重复上述签名过程直至数字签名次数等于预先设定的签名次数N，得到加密字节流S2；
步骤B：从所述加密字节流S2中选取一个字节，转换为数值a，并将该字节从S2中删除；
步骤C：执行取余操作：i＝a％动态密码字符库的长度，其中所述动态密码字符库包括用于生成动态密码的多个字符；
步骤D：从所述动态密码字符库中选取第i个字符，补进动态密码；
步骤E：判断动态密码的长度是否达到要求
否
是
结束动态密码的生成

图 1

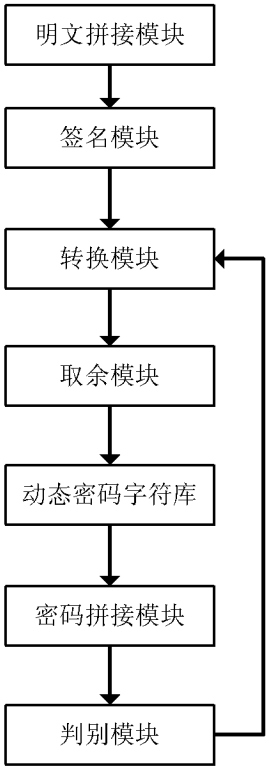



图 2