(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 106817217 B
(45)授权公告日 2019.06.28

(21)申请号 201710046346.9

(22)申请日 2017.01.22

(65)同一申请的已公布的文献号
申请公布号 CN 106817217 A

(43)申请公布日 2017.06.09

(73)专利权人 石家庄科林电气股份有限公司
地址 050222 河北省石家庄市红旗大街南降壁路段(南院)

(72)发明人 张向平 陈贺 陈洪雨 张奎仲 赵鹏 杜宝瑞 赵宏杰 李峥 张权 常生强 李春海 强建龙 郝立佳 李伟

(74)专利代理机构 石家庄众志华清知识产权事务所(特殊普通合伙) 13123
代理人 墨伟

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101163014 A,2008.04.16,
CN 101166091 A,2008.04.23,
US 2013/0124292 A1,2013.05.16,
CN 102752110 A,2012.10.24,

审查员 李锦玲

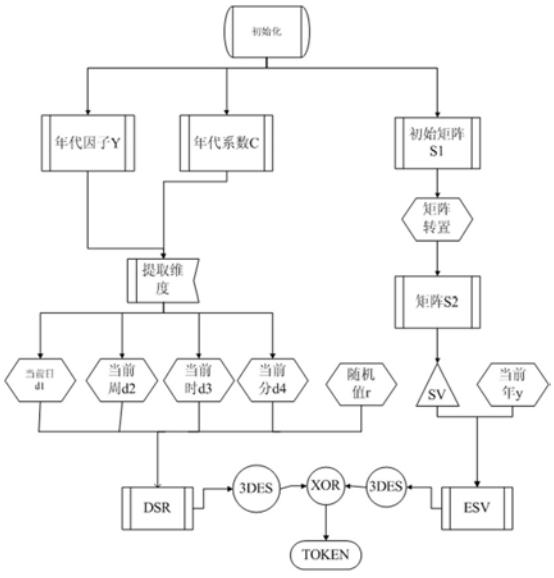
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种分级时效的动态口令加密算法

(57)摘要

本发明公开了一种分级时效的动态口令加密算法,其包括基于时间信息生成的DSR字符串和基于ASCII字符集和时间信息生成的字符串ESV,将字符串DSR与字符串ESV进行长度比较,不足者左侧用0补齐后进行异或运算,将结果记为T,并将T按16进制格式转换成字符串作为动态口令token。其中字符串DSR的生成基于随机指定的年代因子、并依赖于当前日期和/或时刻。从当前日期和时刻提取不同时间维度,通过选取不同的时间维度并与随机值、年代指数、年代系数乱序排列生成字符串并加密。字符串ESV的生成基于ASCII字符集,经过乱序转换矩阵的转换、与年代指数组合生成字符串加密。经过多层加密和乱序转换,增强加密强度。



CN 106817217 B

1.一种分级时效的动态口令加密算法,其特征在于包括以下步骤:

S1、基于时间信息生成DSR字符串

S101、设置年代因子Y,其值在0和15之间,记为Y=[0,15],

S102、系统获取当前日期和时刻,提取当前年y_i、指定基准年y_0,每16年为一个步长,计算当前年的年代指数$y=(y_i- y_0-Y)\%16$,设置年代系数C,其值在0和255之间,$C=(y_i- y_0-Y)/16$,取整,

S103、计算该日期在全年中是第几天,记为d1,计算该日期是一周中的第几天,记为d2,取当前小时时间,记为d3,取当前分钟值,记为d4,

S104、产生随机数R,将随机数R进行6位长度字符串格式化运算,记为r,

S105、选择r、y和C,并与d1、 d2、d3或d4中一个或两个以上按设定规则组合排列,并进行3DES加密,生成字符串DSR;

S2、基于ASCII字符集生成字符串ESV

S201、从ASCII字符集中选取64个字符作为密码集S1,记为$S1=\{s0,s1\cdots s63\}$,

S202、设置0-63乱序排列的转换矩阵V,对密码集S1进行矩阵转换,记为密码集S2,

S203、从密码集S1中取字符串序列转换成密码集S2中的字符生成字符串SV ,并按照设定的规则与步骤S102中当前年的年代指数y值排序,然后进行3DES加密,生成字符串ESV;

S3、将字符串DSR与字符串ESV进行长度比较,不足者左侧用0补齐后进行异或运算,将结果记为T,并将T按16进制格式转换成字符串作为动态口令token,记为t。

2.根据权利要求1所述的分级时效的动态口令加密算法,其特征在于步骤S102中以2000年为基准年。

3.根据权利要求1所述的分级时效的动态口令加密算法,其特征在于步骤S105中选取r、y、C、d1、d2、d3和d4按设定规则排列。

4.根据权利要求1所述的分级时效的动态口令加密算法,其特征在于步骤S105中选取r、y、C、d1和d3 按设定规则排列。

5.根据权利要求1所述的分级时效的动态口令加密算法,其特征在于步骤S203中字符串SV按照设定的规则与步骤S102中当前年的年代指数y值和年代因子C值排序。

一种分级时效的动态口令加密算法

技术领域

[0001] 本发明属于信息安全技术领域，涉及电力系统无线通信数据认证、电动汽车充电管理云平台认证终端或物联网设备接入数据认证，具体涉及一种分级时效的动态口令加密算法。

背景技术

[0002] 在国外，动态口令与基于PKI数字证书的认证技术相比具有使用方便、成本低、免维护、应用面广等优点，在金融、政府、制造业等众多领域得到大量成功应用。在国内，随着国内网上交易爆炸式增长，安全问题日益突出，动态密码的优点越来越受到人们的青睐。

[0003] 动态口令作为目前最安全的身份认证技术之一，已经被越来越多的行业所应用。动态口令具有使用便捷、平台无关等特性，随着移动互联网的发展，动态口令技术被广泛应用于企业、金融、电子商务、物联网等领域。但是，由于互联网的开放性，它不受时空限制，也极易遭受恶意攻击和入侵，因此网络安全保护成为互联网时代一个不可或缺的话题，在网络强国战略写入“十三五“规划这一大背景下，我国首部《网络安全法》已经于2016年11月发布。

[0004] 在互联网应用中，身份认证、访问控制、数据加密、防篡改、防抵赖是安全保护的几个基本要素，身份认证是第一道防线，也是最重要的一道防线，近年来基于身份认证的安全技术发展很快，其中比较成熟的是基于PKI数字证书和动态密码技术。动态密码可方便地与静态PIN码、SSL加密传输等安全技术结合，具有经济、安全的特点，因而被广泛应用于远程身份认证和安全交易支付中。传统的动态口令方法都是基于时间同步的动态口令，对标准时间用口令生成密钥(公钥) 加密生成动态口令。

[0005] 但是，对于电力系统认证交互过程中对于一些特殊权限操作，需要登录人员进行二次口令验证的情况，在取得合法登录身份后，使用动态口令在一定时效范围内进行有限制的功能操作，因此需要对动态口令进行时效分级，比如在小时级范围内进行操作或者在分钟级范围进行操作，即通过不同时效的动态口令达到控制权限操作的目的。

发明内容

[0006] 本发明要解决的技术问题是提供一种分级时效的动态口令加密算法，其从当前日期和时刻提取不同的时间维度，通过选取时间维度的组合，支持时效分级控制，支持不同的时间维度组合方案和时效验证控制，防止伪造，增强加密强度。

[0007] 为解决上述技术问题，本发明采用的技术方案是：

[0008] 一种分级时效的动态口令加密算法，包括以下步骤：

[0009] S1、基于时间信息生成DSR字符串

[0010] S101、设置年代因子Y，其值在0和15之间，记为Y=[0,15]，

[0011] S102、系统获取当前日期和时刻，提取当前年y_i、指定基准年y_0，每16年为一个步长，计算当前年的年代指数$y=(y_i- y_0-Y)\%16$，设置年代系数C，其值在0和255之间，$C=(y_i-y_0-Y)/16$，取整，

[0012] S103、计算该日期在全年中是第几天，记为d1，计算该日期是一周中的第几天，记为d2，取当前小时时间，记为d3，取当前分钟值，记为d4，

[0013] S104、产生随机数R，将随机数R进行6位长度字符串格式化运算，记为r，

[0014] S105、选择r、y和C，并与d1、d2、d3或d4中一个或两个以上按设定规则组合排列，并进行3DES加密，生成字符串DSR；

[0015] S2、基于ASCII字符集生成字符串ESV

[0016] S201、从ASCII字符集中选取64个字符作为密码集S1，记为$S1=\{s0,s1\cdots s63\}$，

[0017] S202、设置0-63乱序排列的转换矩阵V，对密码集S1进行矩阵转换，记为密码集S2，

[0018] S203、从密码集S1中取字符串序列转换成密码集S2中的字符生成字符串SV，并按照设定的规则与步骤S102中当前年的年代指数y值排序，然后进行3DES加密，生成字符串ESV；

[0019] S3、将字符串DSR与字符串ESV进行长度比较，不足者左侧用0补齐后进行异或运算，将结果记为T，并将T按16进制格式转换成字符串作为动态口令token，记为t。

[0020] 上述技术方案中，字符串DSR的生成基于随机指定的年代因子、并依赖于当前日期和/或时刻。从当前日期和时刻提取不同时间维度，通过选取不同的时间维度并与随机值、年代指数、年代系数乱序排列生成字符串并加密。字符串ESV的生成基于ASCII字符集，经过乱序转换矩阵的转换、与年代指数组合生成字符串加密。经过多层加密和乱序转换，增强加密强度。

[0021] 采用上述技术方案产生的有益效果在于：(1)本发明自定义矩阵转换字符串密码表，增强加密强度；(2)使用年代因子、年代系数和年代指数，指定基准时间，时间跨度多达4000年；(3)引入随机数概念，支持不同时间维度组合；(4)引入当前日期天数和星期概念，通过时间维度分级，对口令实现时效管理；(5)使用两组不同的3DES加密机制，支持系统级和终端节点分别加密；(6)具备时间因子和时间系数的自我校验功能；(7)token根据密钥强度，支持简单、中度、复杂等级别，用户可以选择适合自己的加密方式。

附图说明

[0022] 图1是本发明动态口令加密的流程图。

具体实施方式

[0023] A、基于时间信息生成DSR字符串

[0024] S101、设置年代因子Y，其值在0和15之间，记为Y=[0,15]，不同的用户可以自由指定年代因子Y值，本实施例中设置年代因子Y=10。

[0025] S102、系统计算获取当前日期和时刻，提取当前年y_i、指定基准年y_0，每16年为一个步长，计算当前年的年代指数$y=(y_i- y_0-Y)\%16$。并设置年代系数C，其值在0和255之间，$C=(y_i- y_0-Y)/16$，取整。每16年为一个步长，年份每增加16年，年代系数C加1，该方法可以用于的时间跨度多达4000年。$y=(y_i- y_0) -Y-16\times C$，支持时效验证。

[0026] 比如，当天日期为2016年11月11日，指定基准年y_0=2000年，则根据$(y_i- y_0-Y)/16$计算，其整数为年代系数C，余数为当前年的年代指数，本实施例中C=0，y=6。

[0027] S103、计算该日期在全年中是第几天，记为d1，计算该日期是一周中的第几天，记

为d2,取当前小时时间,记为d3,取当前分钟值,记为d4。

[0028] 由2016年11月11日,可以计算该日为一年中的第316天,即d1=316,当天是周五,即d2=6(周日、周一到周六分别对应1-7),时间是14:30分,则d3=14,d4=30。

[0029] S104、产生随机数R,将随机数R进行6位长度字符串格式化运算,记为r。

[0030] 设r="12345"。

[0031] S105、选择r、y和C,并与d1、d2、d3或d4中一个或两个以上按设定规则组合排列,并进行3DES加密,生成字符串DSR。

[0032] 本实施例中选择d1、d2、d3和d4与r、y和C按照r-d1-d3-d4-d2-C-y的方式组合,则有字符串"123453161430060006",并将该字符串进行3DES加密,生成字符串DSR。

[0033] S2、基于ASCII字符集生成字符串ESV

[0034] S201、从ASCII字符集中选取64个字符作为密码集S1,记为$S1=\{s0,s1\cdots s63\}$,

[0035] 本实施例设置密码集S1=

[0036] { A B C D E F G H }

[0037] { I J K L M N O P }

[0038] { Q R S T U V W X }

[0039] { a b c d e f g h }

[0040] { i j k o p q r s }

[0041] { t u v x z 1 2 3 }

[0042] { 4 5 6 7 8 9 0 ! }

[0043] { @ # $ % ^ & * (}

[0044] S202、设置0-63乱序排列的转换矩阵V,对密码集S1进行矩阵转换。

[0045] 本实施例设置乱序排列的转换矩阵V=

[0046] { 50 4 20 28 8 30 17 35 }

[0047] { 3 27 21 36 1 9 29 46 }

[0048] { 48 16 0 5 13 37 18 11 }

[0049] { 26 49 7 23 33 2 10 38 }

[0050] { 51 24 14 22 52 34 39 19 }

[0051] { 25 41 53 56 40 32 12 6 }

[0052] { 31 42 15 44 61 63 60 47 }

[0053] { 55 54 59 43 57 45 58 62 }

[0054] 则有密码集S2=

[0055] { S M f I B T 3 c }

[0056] { E N g X 2 U k 6 }

[0057] { R G W s C K o d }

[0058] { j t a J D O F 4 }

[0059] { 1 e q H L V h r }

[0060] { z u 5 % 7 & P ! }

[0061] { Q b A i p v # @ }

[0062] { x ^ * $ 0 8 (9 }

[0063] S203、从密码集S1中取字符串序列转换成密码集S2中的字符生成字符串SV，并按照设定的规则与步骤S102中当前年的年代指数y值排序，然后进行3DES加密，生成字符串ESV。

[0064] 本实施例中设有字符串“PiNg1978”，转换后得SV为“61UF&vip”，增加步骤S102中当前年的年代指数y=6，得到字符串“61UF&vip0006”，将该步骤中的字符串进行3DES加密转化，生成字符串ESV。

[0065] 在其它实施例中字符串SV还可以按照设定的规则与步骤S102中当前年的年代指数y值和年代因子C值进行排序。

[0066] S3、将字符串DSR与字符串ESV进行长度比较，不足者左侧用0补齐后进行异或运算，将结果记为T，并将T按16进制格式转换成字符串作为动态口令token，记为t。

[0067] 本实施例中将T转为16进制字符串，得“ASE4343334dd454”。

[0068] 综上所述，本发明采用两维度矩阵加密技术，基于时间的动态口令，支持分级控制，支持不同的时间维度组合方案，支持不同的时效验证控制，具备时间因子和时间系数的自我校验功能，防伪造。

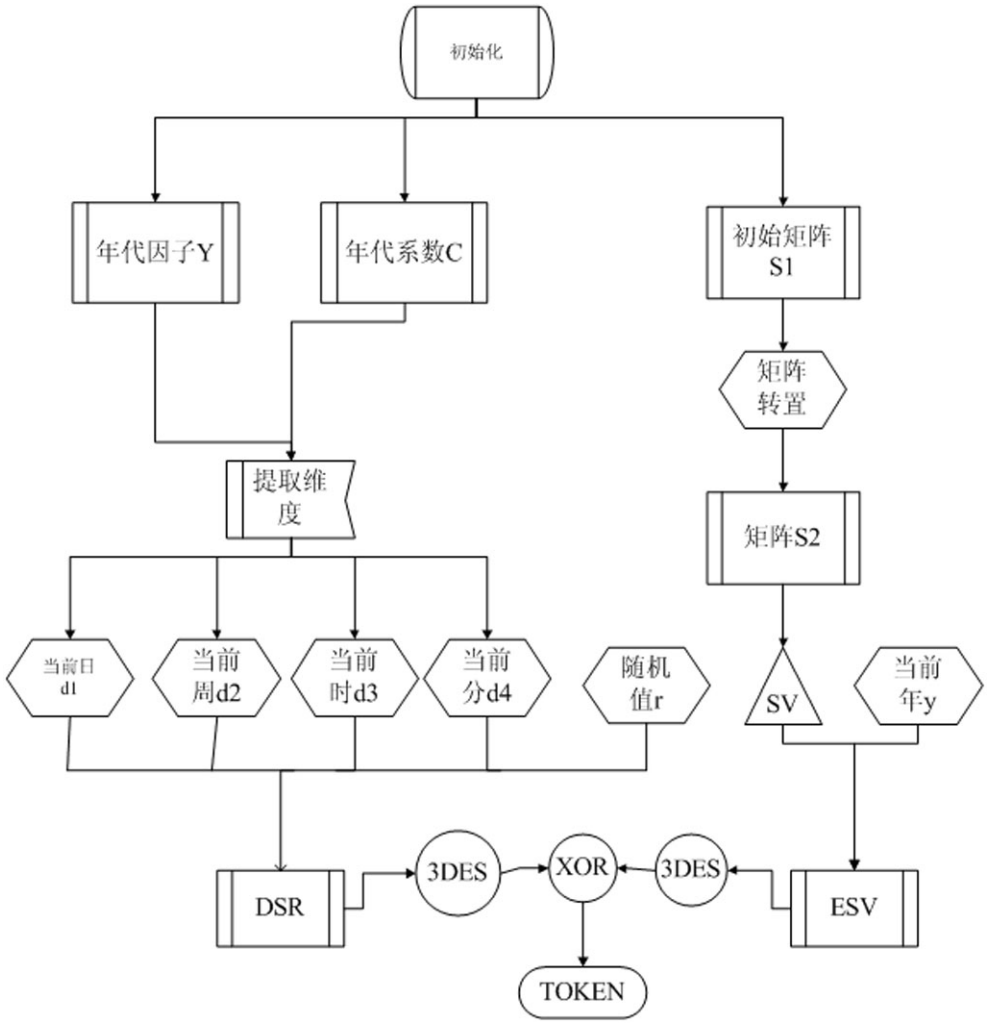

初始化
年代因子Y
年代系数C
初始矩阵S1
矩阵转置
提取维度
矩阵S2
当前日d1
当前周d2
当前时d3
当前分d4
随机值r
SV
当前年y
DSR
3DES
XOR
3DES
ESV
TOKEN

图1