(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 103731270 B
(45)授权公告日 2017.02.08

(21)申请号 201310737247.7

(22)申请日 2013.12.25

(65)同一申请的已公布的文献号
申请公布号 CN 103731270 A

(43)申请公布日 2014.04.16

(73)专利权人 华南理工大学
地址 510640 广东省广州市天河区五山路381号

(72)发明人 谢宗伯 蔡琳琳 冯久超

(74)专利代理机构 广州市华学知识产权代理有限公司 44245
代理人 蔡茂略

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)

(56)对比文件
CN 202404689 U,2012.08.29,
CN 101188493 A,2008.05.28,
CN 101605326 A,2009.12.16,
CN 103401678 A,2013.11.20,
WO 2008018042 A2,2008.02.14,

审查员 张秀娟

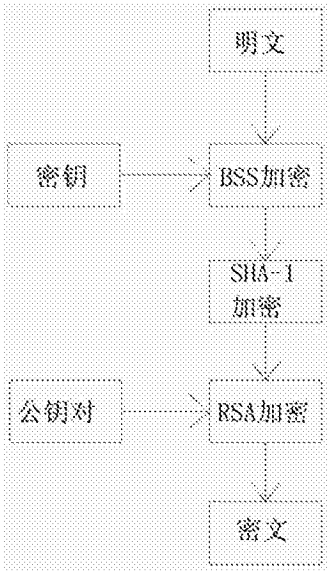
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法

(57)摘要

本发明公开了一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，其步骤为：1)生成待加密发送的数据；2)将待发送的数据进行第一次加密，即进行BSS加密；3)对完成第一次加密的数据使用SHA-1加密算法生成摘要内容；4)利用接收端提供的RSA加密公钥对经过SHA-1加密的数据以及摘要进行加密；5)发送密文；6)接收端接收密文并利用自身的私钥对密文进行第一次解密；7)对接收到的数据进行身份认证；8)对完成身份认证的数据进行BSS解密，读取数据内容。本发明利用三种加密算法的不同特点，将待发送的消息分别经过BSS、SHA-1以及RSA算法的加密，使得用于通信的加密信息更加安全，并且实现数字签名，用于保证收到的信息为发送端发送的原始信息，而没有受到篡改。



CN 103731270 B

1.一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，其特征在于，包括以下步骤：

1)获取待加密发送的数据；

2)将待发送的数据进行第一次加密，即进行BSS加密；

3)对完成第一次加密的数据使用SHA-1加密算法生成摘要内容；

4)利用接收端提供的RSA加密公钥对经过BSS加密的数据以及经过SHA-1加密算法生成的摘要进行加密；其中，在进行RSA加密前，先查看发送端是否有接收端的含有RSA加密公钥的数字证书，有则进行RSA加密，否则，则暂停加密，而改为向接收端发送数字证书请求消息；

5)发送密文；

6)接收端接收密文并利用自身的私钥对密文进行第一次解密；

7)对接收到的数据进行身份认证：首先对进行第一次解密后的数据中除开摘要部分的其它所有数据进行SHA-1运算，形成新的一个摘要，然后将得到的摘要与接收到的摘要进行对比，如有不同，则说明数据被人篡改过，丢弃数据，否则，转至步骤8)；

8)对完成身份认证的数据进行BSS解密，读取数据内容；其中，在进行BSS解密前，先查看接收端是否有发送端的有效数字证书，有则直接进行BSS解密，否则暂停解密，转而向发送端发送数字证书请求消息，然后从数字证书中解密出BSS密钥种子，生成BSS解密密钥信号来完成解密。

2.根据权利要求1所述的一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，其特征在于：所述数字证书包含用户ID、RSA公钥对、BSS密钥种子、证书启用时间、证书停用时间，其中，所述RSA公钥对存放的是接收端自身的RSA公钥对；所述BSS密钥种子存放的是发送端自身的密钥种子，所述BSS密钥种子是经过SHA-1身份认证加密以及使用接收端中所存储的RSA公钥对进行RSA加密。

一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法

技术领域

[0001] 本发明涉及移动终端收发数据的加解密流程的技术领域，尤其是指一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法。

背景技术

[0002] 随着社会的发展，移动终端的功能越来越强悍，各种公司企业提供的业务也越来越多种多样，大大的方便了人们的生活。但是，伴随而来的就是信息安全的问题。例如现在人们会通过移动终端来传送账号密码等信息，有许多的不法之徒就会采用恶意攻击等手段来截获用户的有用信息以求牟利。本发明提出的移动终端的加密流程是基于以下三个的技术的。

[0003] BSS加密方法：1)BSS(盲源分离)及其欠定问题：假设存在M个独立的源信号S_1，S_2，…，S_M，以及N个可观察的混合信号X_1，X_2，…，X_N，(一般N≥M)，线性BSS混合模型混合方程为X＝AS，其中S＝(S_1，S_2，…，S_M)^T，A为一个N×M矩阵。BSS的目的就是寻找一个M×N矩阵恢复出一个M×1信号矩阵。当源信号大于观察混合信号，即N≤M时，BSS就变成了一个困难的欠定问题，此时想要源信号完全分离是不可能的。2)BSS加密方法是基于解决欠定BSS问题的困难性来实现的。将要加密的数据分帧进行加密，每一帧信号分成P段为s_1，s_2，…，s_p，每段长度为T。利用参数密钥种子I生成P个独立的密钥信号s_{n1}，s_{n2}，…，s_{np}。然后生成2P欠定混合矩阵A_ϕ。然后P个源信号段和P个密钥信号一起在欠定混合矩阵的作用下，生成P个加密了的信号x_1，x_2，…，x_p。生成方程为X＝A_ϕ×S，其中S＝(s_1，s_2，…，s_p，s_{n1}，s_{n2}，…，s_{np})^T，X＝(x_1，x_2，…，x_p)^T。可以看出，有2P个源信号，但是只有P个混合信号，这样的加密过程就把BSS问题变成了欠定的BSS问题。在解密端，只有在知道密钥种子I，生成P个独立密钥s_{n1}，s_{n2}，…，s_{np}，与X联合变成用于解密的X_d＝(x_1，x_2，…，x_p，s_{n1}，s_{n2}，…，s_{np})^T，那么X_d＝A_d×S_d，其中A_d为2P×2P矩阵。可以看出，在解密阶段，由于有了密钥，源信号和混合信号数量相等了，则把加密阶段产生的BSS欠定问题变成了正常的BSS问题，那么就可以用BSS将源信号给恢复出来。

[0004] SHA-1加密算法：SHA是美国国家标准和技术局发布的国家标准。SHA-1是SHA家族中应用最为广泛的一个算法。SHA-1算法对输入的报文长度不限，然后将输入的明文按照512位(64个字节)每组进行分块，经过一种不可逆的散列运算产生一组160位(20字节)的报文摘要。由于SHA-1的散列算法有不可逆性和良好的雪崩效应，所以不可能从散列结果推导出任何的原始数据，并且也原始数据任何的改变，哪怕一位，都会造成散列结果的差异。将要传送的明文和报文摘要一起发送给接收方，接收方利用收到的明文产生相应的报文摘要，将产生的报文摘要与接收到的报文摘要进行比较，如果相同说明明文没有被篡改，否则就是中间被人篡改了。

[0005] RSA加密算法：RSA是一种非对称加密算法，即有公钥和私钥两种密钥。发送方利用接收方提供的公共密钥来对数据加密，接收方就用自己拥有的私钥对信息进行解密。因为公钥和私钥是一一对应的，所以只有拥有私钥的接收方才能解密用它提供的公钥加密的数据。并且RSA算法是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”安全体制，

这也保证了加密数据的安全性。

发明内容

[0006] 本发明的目的在于克服现有技术的不足与缺陷，提供一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，不但使得移动终端传输的加密数据更加安全，而且实现了数字签名，使得数据更具有不可抵赖性。

[0007] 为实现上述目的，本发明所提供的技术方案为：一种基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，包括以下步骤：

[0008] 1)获取待加密发送的数据；

[0009] 2)将待发送的数据进行第一次加密，即进行BSS加密；

[0010] 3)对完成第一次加密的数据使用SHA-1加密算法生成摘要内容；

[0011] 4)利用接收端提供的RSA加密公钥对经过BSS加密的数据以及经过SHA-1加密算法生成的摘要进行加密；

[0012] 5)发送密文；

[0013] 6)接收端接收密文并利用自身的私钥对密文进行第一次解密；

[0014] 7)对接收到的数据进行身份认证；

[0015] 8)对完成身份认证的数据进行BSS解密，读取数据内容。

[0016] 在步骤4)中，在进行RSA加密前，先查看发送端是否有接收端的含有RSA加密公钥的数字证书，有则进行RSA加密，否则，则暂停加密，而改为向接收端发送数字证书请求消息。

[0017] 在步骤7)中，对收到的数据进行身份认证的过程为：首先对进行第一次解密后的数据中除开摘要部分的其它所有数据进行SHA-1运算，形成新的一个摘要，然后将得到的摘要与接收到的摘要进行对比，如有不同，则说明数据被人篡改过，丢弃数据，否则，转至步骤8)。

[0018] 在步骤8)中，在进行BSS解密前，先查看接收端是否有发送端的有效数字证书，有则直接进行BSS解密，否则暂停解密，转而向发送端发送数字证书请求消息，然后从数字证书中解密出BSS密钥种子，生成BSS解密密钥信号来完成解密。

[0019] 所述数字证书包含用户ID、RSA公钥对、BSS密钥种子、证书启用时间、证书停用时间，其中，所述RSA公钥对存放的是接收端自身的RSA公钥对；所述BSS密钥种子存放的是发送端自身的密钥种子，所述BSS密钥种子是经过SHA-1身份认证加密以及使用接收端中所存储的RSA公钥对进行RSA加密。

[0020] 本发明与现有技术相比，具有如下优点与有益效果：

[0021] 1、对于一般的数据加密，基本都是只进行对称加密或者非对称加密中的一种，而本发明同时使用了对称加密和非对称加密两种形式的加密方法，所以使得数据具有更高的安全性；

[0022] 2、本发明对数据进行加密的同时，还进行了数字签名，这样在对数据加密的同时，也保证了加入数据不行被篡改，也不会因为篡改的信息而遭受损失，进而很好地预防恶意篡改数据带来的危害。

附图说明

[0023] 图1为本发明在加密阶段的流程图。

[0024] 图2为本发明在解密阶段的流程图。

具体实施方式

[0025] 下面结合具体实施例对本发明作进一步说明。

[0026] 本实施例所述的基于BSS、RSA、SHA-1加密算法的通信数据加解密方法，其具体情况如下：

[0027] 1)获取待加密发送的数据；

[0028] 2)将待发送的数据进行第一次加密，即进行BSS加密；

[0029] 3)对完成第一次加密的数据使用SHA-1加密算法生成摘要内容；

[0030] 4)利用接收端提供的RSA加密公钥对经过BSS加密的数据以及经过SHA-1加密算法生成的摘要进行加密；

[0031] 5)发送密文；

[0032] 6)接收端接收密文并利用自身的私钥对密文进行第一次解密；

[0033] 7)对接收到的数据进行身份认证；

[0034] 8)对完成身份认证的数据进行BSS解密，读取数据内容。

[0035] 在步骤4)中，在进行RSA加密前，先查看发送端是否有接收端的含有RSA加密公钥的数字证书，有则进行RSA加密，否则，则暂停加密，而改为向接收端发送数字证书请求消息。

[0036] 在步骤7)中，对收到的数据进行身份认证的过程为：首先对进行第一次解密后的数据中除开摘要部分的其它所有数据进行SHA-1运算，形成新的一个摘要，然后将得到的摘要与接收到的摘要进行对比，如有不同，则说明数据被人篡改过，丢弃数据，否则，转至步骤8)。

[0037] 在步骤8)中，在进行BSS解密前，先查看接收端是否有发送端的有效数字证书，有则直接进行BSS解密，否则暂停解密，转而向发送端发送数字证书请求消息，然后从数字证书中解密出BSS密钥种子，生成BSS解密密钥信号来完成解密。

[0038] 由于本发明同时采用了DES加密和RSA加密两种方式，涉及到密钥的传送问题，这里提出了一种新的数字证书内容，如下表所示：

[0039]

用户ID	RSA公钥对	BSS密钥种子	证书启用时间	证书停用时间

[0040] 其中，RSA公钥对存放的是接收端自身的RSA公钥对，BSS密钥种子存放的是发送端自身的密钥种子。数字证书中存储的BSS密钥种子并非直接的BSS密钥种子而是经过了SHA-1身份认证加密以及使用接收端数字证书中所存储的RSA公钥对进行了RSA加密，这样就保证了BSS密钥种子的安全。所以接收端要使用BSS密钥种子时，必须先用自身的RSA密钥进行解密以及身份验证后才可以使用。

[0041] 本实施例所述的发送端包括有加密模块、密钥存储模块、发送模块，所述的接收端包括有数据获取模块、显示模块、缓存模块、接收模块。其中，所述密钥存储模块里存放着自

身的用于BSS加密的密钥种子、RSA解密私钥对，其它终端的数字证书。

[0042] 如图1所示，在加密阶段，数据获取模块得到数据后，首先将数据分成一帧一帧的，然后将每一帧分成P段，以及得到段长T，提取出P和T。从密钥存储模块得到密钥种子，与P、T相结合生成BSS加密密钥，然后对数据进行BSS加密，每一帧得到的密文结果先缓存在缓存模块中，然后将所有明文产生的总的密文进行SHA-1加密得到一个摘要。

[0043] 得到报文摘要的密文和摘要一起进行RSA加密，在进行RSA加密前，发送端先检查自己的密钥存储模块是否有接收端的数字证书以及数字证书是否过期，如果有且在使用期内，则继续进行，如果没有所需数字证书或者已经过期，则把密文和摘要放到缓存模块中，转而向接收端发送数字证书请求消息。得到接收端的数字证书后，利用其中的RSA加密公钥对，对经过一轮加密的密文和摘要进行RSA加密，得到最终的密文，然后从发送模块发送出去。

[0044] 如图2所示，在解密阶段，接收模块接受到密文后，首先对其进行RSA解密。进行RSA解密时，接收端调用自己RSA私钥对，只有和发送端使用的公钥对是适配的私钥对才可以正确地对密文进行解密。

[0045] 完成RSA解密的数据分为两个部分：一部分是报文摘要S1，另一部分是进过了BSS加密的密文。对密文进行重新一轮的SHA-1运算，得到另外一个报文摘要S2，然后将得到的报文摘要S2与原来的报文摘要S1进行比较，如果完全一致，则说明数据没有被篡改，可以继续下面的解密，如果有任何出入，则说明有被改动，把得到的数据丢弃，并且向发送端发送警报信号。

[0046] 完成身份认证的数据将进行最后的BSS解密，在BSS解密前，接收端先检查自己的密钥存储模块是否有发送端的数字证书并且是否在使用期内。如果有且在有效期内，则直接进行BSS解密，如果没有需要的数字证书或者已经过期，则将数据暂时放入缓存模块，转而向发送端发送数字证书请求消息。得到发送端的数字证书后，利用其中的BSS密钥种子生成BSS解密密钥，然后对数据进行最后的解密，得到最后所需的明文。

[0047] 以上所述之实施例子只为本发明之较佳实施例，并非以此限制本发明的实施范围，故凡依本发明之形状、原理所作的变化，均应涵盖在本发明的保护范围内。

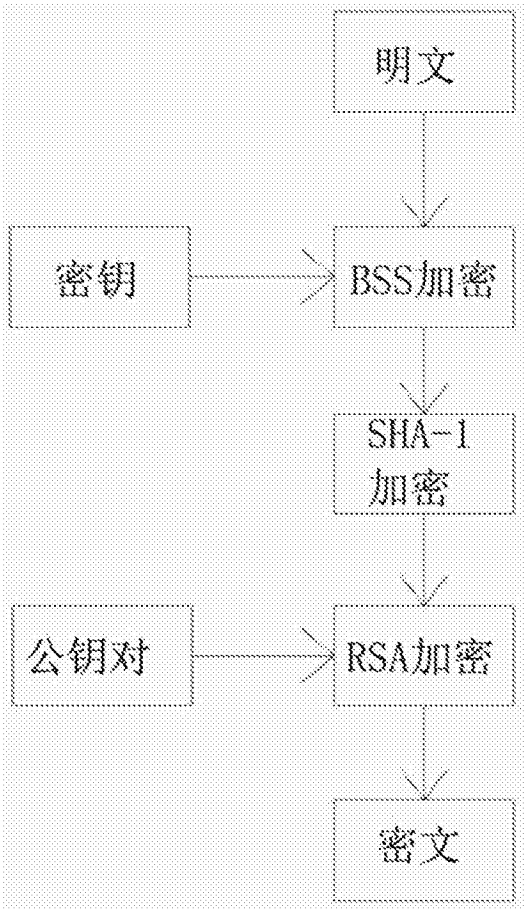


图1

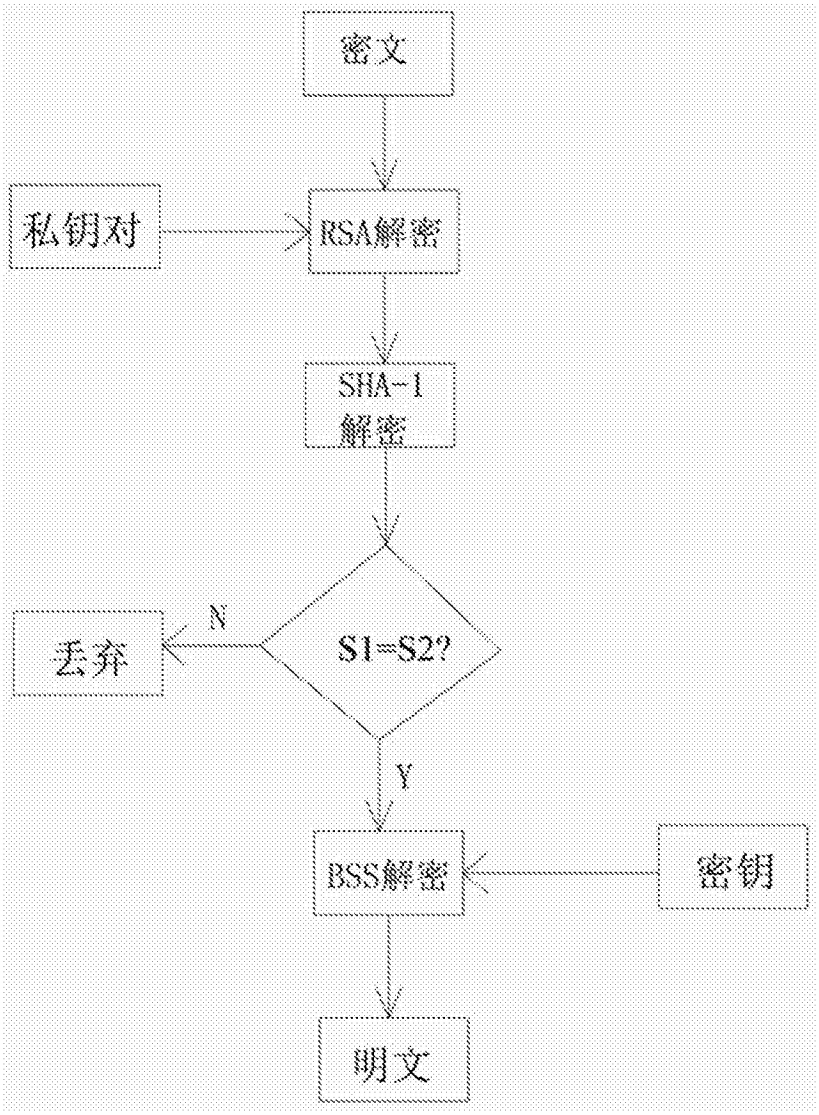


图2