(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 102904712 B
(45)授权公告日 2016.01.06

(21)申请号 201110208448.9
(22)申请日 2011.07.25
(73)专利权人 深圳市金溢科技股份有限公司
地址 518057 广东省深圳市南山区科苑路清华信息港研发楼A栋12层
(72)发明人 王政 吴恒志 林树亮
(74)专利代理机构 深圳市铭粤知识产权代理有限公司 44304
代理人 杨林
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
CN 101335616 A,2008.12.31,
CN 101226705 A,2008.07.23,
CN 102073831 A,2011.05.25,
US 2004101142 A1,2004.05.27,
US 6490353 B1,2002.12.03,
审查员 孟维志

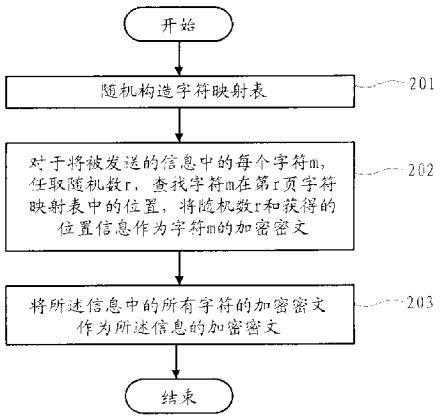
权利要求书2页 说明书6页 附图4页

(54)发明名称

信息加密方法

(57)摘要

本发明提供一种信息加密方法，所述方法包括：随机构造字符映射表，所述字符映射表包含多页，每页字符映射表包含所有ASCII码字符，每个ASCII码字符在每页字符映射表中出现至少一次；对于将被发送的信息中的每个字符m，任取随机数r，0≤r≤字符映射表的页数，查找所述字符m在第r页字符映射表中的位置，将随机数r和获得的位置信息作为所述字符m的加密密文；将所述信息中的所有字符的加密密文作为所述信息的加密密文。本发明采用强大的密钥配以简单的算法，主要解决信息在传输过程中被非法截获而被还原的问题。



CN 102904712 B

1. 一种信息加密方法，包括：

(a) 随机构造字符映射表，所述字符映射表包含多页，每页字符映射表包含所有 256 个 ASCII 码字符，每个 ASCII 码字符在每页字符映射表中只出现一次；

(b) 对于将被发送的信息中的每个字符 m，任取随机数 r，0 ≤ r ≤字符映射表的页数，查找所述字符 m 在第 r 页字符映射表中的位置，将随机数 r 和获得的位置信息作为所述字符 m 的加密密文；

(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文，

其中，随机构造字符映射表的步骤包括：

(a1) 对于每页字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255，将字符映射表中第 R1 个字符与第 R2 个字符交换；

(a2) 重复执行步骤 (a1) 预定次数。

2. 根据权利要求 1 所述的信息加密方法，其特征在于：在解密过程中，依次读取所述信息的加密密文，获得关于每个字符 m 的随机数 r 以及所述字符 m 在第 r 页字符映射表中的位置，根据读取的位置信息在第 r 页字符映射表中查找每个字符 m 的原文。

3. 一种信息加密方法，包括：

(a) 随机构造一页字符映射表，所述字符映射表包含所有 256 个 ASCII 码字符，每个 ASCII 码字符在所述字符映射表中只出现一次；

(b) 对于将被发送的信息中的每个字符 m，查找所述字符 m 在字符映射表中的位置，将获得的位置信息作为所述字符 m 的加密密文；

(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文，

其中，随机构造字符映射表的步骤包括：

(a1) 对于所述字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255，将字符映射表中第 R1 个字符与第 R2 个字符交换；

(a2) 重复执行步骤 (a1) 预定次数。

4. 根据权利要求 3 所述的信息加密方法，其特征在于：在解密过程中，依次读取所述信息的加密密文，获得每个字符 m 在字符映射表中的位置，根据读取的位置信息在字符映射表中查找每个字符 m 的原文。

5. 一种信息加密方法，包括：

(a) 随机构造一页字符映射表，所述字符映射表包含所有 256 个 ASCII 码字符，每个 ASCII 码字符在所述字符映射表中只出现一次；

(b) 对于将被发送的信息中的每个字符 m，字符 m 所对应的 ASCII 码的十进制值为 x，所述字符映射表中第 x 个字符为字符 n，将字符 m 映射为字符 n，作为所述字符 m 的加密密文；

(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文，

其中，随机构造字符映射表的步骤包括：

(a1) 对于所述字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255，将字符映射表中第 R1 个字符与第 R2 个字符交换；

(a2) 重复执行步骤 (a1) 预定次数。

6. 根据权利要求 5 所述的信息加密方法，其特征在于：在解密过程中，首先构造解密字

符映射表，

构造解密字符映射表的步骤包括：对于字符映射表中的每一个字符 a，字符 a 的 ASCII 码的十进制值为 y，字符映射表中第 y 个字符为字符 b，将字符 b 布置在解密字符映射表的第 y 个位置，由此构造解密字符映射表，

在解密时，依次读取所述信息的加密密文，获得加密密文中的每个字符在解密字符映射表中的位置 z，将 z 值所对应的 ASCII 码字符作为解密的原文。

7. 根据权利要求 1、3、5 中任一项所述的信息加密方法，其特征在于：字符映射表和 / 或加密解密算法代码存储在各个通信节点的安全模块中。

8. 根据权利要求 1、3、5 中任一项所述的信息加密方法，其特征在于：随机构造字符映射表的步骤还包括，

(a3) 将字符映射表与预定的分散因子进行分散运算。

信息加密方法

技术领域

[0001] 本发明涉及数据加密技术领域，更具体地讲，本发明涉及一种利用字符映射表的信息加密方法，属于对称密钥的加密方法。

背景技术

[0002] 数据加密方法一般分为对称密钥加密方法和非对称密钥（公开密钥）加密方法两种。随着现代通信信息量不断加大，人们对数据安全的认识和要求越来越高。为了保证传输过程中通信内容不会泄密，可供使用的数据加密传输方法有很多。由于公知的非对称密钥方法（如 RSA，ECC 等）计算强度太大，因此并不适合大数据量通信时使用，相对而言对称密钥加密方法更适合一些。常用的对称密钥加密方法有 DES、AES 等标准公开的算法，但是这些公开算法的计算量非常大，加密和解密的时间成本很高，也不利于大数据量通信的加密。为了提高计算速度，出现了各种基于硬件的 DES 加密芯片，这样系统在提高加密运算速度的同时也增加了系统的经济成本。

[0003] 现有的对称密钥加密方法（包括 DES、AES 以及其它未公开的方法）的一个通常的做法是：强大的算法配以简单的密钥，比如 DES 算法的密钥长度只有 8 字节。这么做的优点是密钥简单且无须花很大的成本存储或记忆，强大的算法使得通过逆运算破解很困难。但是随着技术的发展，计算机运算能力越来越快，使得暴力破解这种加密方法变得越来越简单。如果使用联网的技术加上穷举的办法破解 8 字节密钥的 DES 加密已经是很容易的事情。

[0004] DES 和 AES 算法已经公布多年，随着时间的推移，已经由多种有效破解 DES 和 AES 的方法公布。随着通信量的加大，需要一种高效率、低成本并且高强度的信息加密方法，以支持大数据量通信。

发明内容

[0005] 本发明针对 DES、AES 等方法的不足之处，提供一种高强度、高效率、低成本的对称密钥加密方法。

[0006] 根据本发明的一方面，提供一种信息加密方法，所述方法包括：(a) 随机构造字符映射表，所述字符映射表包含多页，每页字符映射表包含所有 ASCII 码字符，每个 ASCII 码字符在每页字符映射表中出现至少一次；(b) 对于将被发送的信息中的每个字符 m，任取随机数 r，0 ≤ r ≤字符映射表的页数，查找所述字符 m 在第 r 页字符映射表中的位置，将随机数 r 和获得的位置信息作为所述字符 m 的加密密文；(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文。

[0007] 优选地，随机构造字符映射表的步骤可包括：(a1) 对于每页字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ L，0 ≤ R2 ≤ L，L 为每页字符映射表包含的 ASCII 码字符的数量，将字符映射表中第 R1 个字符与第 R2 个字符交换；(a2) 重复执行步骤 (a1) 预定次数。

[0008] 优选地，字符映射表和 / 或加密解密算法代码可存储在各个通信节点的安全模块

中。

[0009] 优选地，随机构造字符映射表的步骤还可包括：(a3) 将字符映射表与预定的分散因子进行分散运算。

[0010] 优选地，在解密过程中，依次读取所述信息的加密密文，获得关于每个字符 m 的随机数 r 以及所述字符 m 在第 r 页字符映射表中的位置，根据读取的位置信息在第 r 页字符映射表中查找每个字符 m 的原文。

[0011] 根据本发明的另一方面，提供一种信息加密方法，所述方法包括：(a) 随机构造一页字符映射表，所述字符映射表包含所有 256 个 ASCII 码字符，每个 ASCII 码字符在所述字符映射表中只出现一次；(b) 对于将被发送的信息中的每个字符 m，查找所述字符 m 在字符映射表中的位置，将获得的位置信息作为所述字符 m 的加密密文；(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文。

[0012] 优选地，随机构造字符映射表的步骤包括，(a1) 对于所述字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255，将字符映射表中第 R1 个字符与第 R2 个字符交换；(a2) 重复执行步骤 (a1) 预定次数。

[0013] 优选地，在解密过程中，依次读取所述信息的加密密文，获得每个字符 m 在字符映射表中的位置，根据读取的位置信息在字符映射表中查找每个字符 m 的原文。

[0014] 优选地，字符映射表和 / 或加密解密算法代码可存储在各个通信节点的安全模块中。

[0015] 优选地，随机构造字符映射表的步骤还可包括：(a3) 将字符映射表与预定的分散因子进行分散运算。

[0016] 根据本发明的另一方面，提供一种信息加密方法，所述方法包括：(a) 随机构造一页字符映射表，所述字符映射表包含所有 256 个 ASCII 码字符，每个 ASCII 码字符在所述字符映射表中只出现一次；(b) 对于将被发送的信息中的每个字符 m，字符 m 所对对应的 ASCII 码的十进制值为 x，所述字符映射表中第 x 个字符为字符 n，将字符 m 映射为字符 n，作为所述字符 m 的加密密文；(c) 将所述信息中的所有字符的加密密文作为所述信息的加密密文。

[0017] 优选地，随机构造字符映射表的步骤包括，(a1) 对于所述字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255，将字符映射表中第 R1 个字符与第 R2 个字符交换；(a2) 重复执行步骤 (a1) 预定次数。

[0018] 优选地，在解密过程中，首先构造解密字符映射表，构造解密字符映射表的步骤包括：对于字符映射表中的每一个字符 a，字符 a 的 ASCII 码的十进制值为 y，字符映射表中第 y 个字符为字符 b，将字符 b 布置在解密字符映射表的第 y 个位置，由此构造解密字符映射表。在解密时，依次读取所述信息的加密密文，获得加密密文中的每个字符在加密字符映射表中的位置 z，将 z 值所对应的 ASCII 码字符作为解密的原文。

[0019] 优选地，字符映射表和 / 或加密解密算法代码可存储在各个通信节点的安全模块中。

[0020] 优选地，随机构造字符映射表的步骤还可包括：(a3) 将字符映射表与预定的分散因子进行分散运算。

[0021] 本发明采用强大的密钥配以简单的算法，主要解决信息在传输过程中被非法截获

而被还原的问题。

附图说明

[0022] 图 1 是根据本发明的数据加密方法的总体框图。

[0023] 图 2 是根据本发明的数据加密方法的总体流程图。

[0024] 图 3 是根据本发明实施例 3 的数据加密方法的加密流程图。

[0025] 图 4 是根据本发明实施例 3 的数据加密方法的解密流程图。

[0026] 图 5 示出了根据本发明实施例 5 的数据加密方法的总体框图。

具体实施方式

[0027] 通过结合附图，从下面的实施例的描述中，本发明这些和 / 或其它方面及优点将会变得清楚，并且更易于理解，其中 ：

[0028] 图 1 是根据本发明的数据加密 / 解密方法的总体框图。如图 1 所示，根据本发明的数据加密方法的主要技术构思包括以下内容。

[0029] 在信息发送方 10，通信节点 A 可包括加密模块 11，加密模块 11 用于对发送的信息进行加密。加密模块 11 可以是软件模块，也可以是硬件模块。加密模块 11 随机生成字符映射表 12，字符映射表 12 的内容随机，字符映射表 12 的长度（即，字符映射表 12 所包含的字符的数量）大于或等于 256，但应包含所有 256 个 ASCII 字符，256 个 ASCII 字符可在字符映射表 12 中出现一次或多次 ；该字符映射表 12 将作为所有信息加密 / 解密的基础。

[0030] 加密模块 11 在信息被发送之前以字符映射表 12 为基础按预定的算法对信息内容进行编码。具体地，加密模块 11 可使用加密算法 Enc(Dict,M) 对需要被加密的信息进行加密，加密算法 Enc(Dict,M) 是一个简单的字符映射函数，具有非常高的时间效率，其中 Dict 为字符映射表 12 的内容，M 为要进行加密的信息内容。信息被加密之后，由通信节点 A 通过通信链路将加密的信息发送到通信节点 B。通信节点 B 可获得加密的信息。

[0031] 在信息接收方 20，通信节点 B 可包括解密模块 21，用于对接收到的加密信息进行解密。解密模块 21 可以是软件模块，也可以是硬件模块。具体地，解密模块 21 使用解密算法 Dec(Dict,M’) 对接收到的加密信息进行解密，解密算法 Dec(Dict,M’) 也是一个简单的字符映射函数，具有非常高的时间效率，其中 Dict 为字符映射表 12 的内容，M’ 为加密后的信息（即，需要进行解密的信息）。解密算法 Dec(Dict,M’) 是加密算法 Enc(Dict,M) 的逆过程。解密模块 21 以字符映射表 12 为基础按所述预定算法 Dec(Dict,M’) 对加密的信息进行解密，由此获得信息的原文内容。

[0032] 图 2 是根据本发明的数据加密方法的总体流程图。

[0033] 参照图 2，在步骤 201，随机构造字符映射表，所述字符映射表可包含多页，每页字符映射表包含所有 ASCII 码字符，每个 ASCII 码字符在每页字符映射表中出现至少一次。

[0034] 在步骤 202，对于将被发送的信息 M 中的每个字符 m，任取随机数 r，0 ≤ r ≤字符映射表的页数，查找字符 m 在第 r 页字符映射表中的位置，将随机数 r 和获得的位置信息作为字符 m 的加密密文。如果字符 m 在第 r 页字符映射表中出现了多次，则可采用字符 m 在第 r 页字符映射表中的多个位置中的任意一个位置作为字符 m 的位置信息。

[0035] 在步骤 203，将获得的所述信息中的所有字符的加密密文作为所述信息的加密密

文。

[0036] 具体地讲，可按照下面的方式来随机构造字符映射表：(1) 对于每页字符映射表的初始内容，任取随机数 R1 和 R2，0 ≤ R1 ≤ L，0 ≤ R2 ≤ L，L 为每页字符映射表包含的 ASCII 码字符的数量（即，每页字符映射表的长度），将字符映射表中第 R1 个字符与第 R2 个字符交换；(2) 重复执行前面的步骤 (1) 预定次数。所述预定次数可以等于或大于 L/2。

[0037] 在解密过程中，依次读取所述信息的加密密文，获得关于每个字符 m 的随机数 r 以及所述字符 m 在第 r 页字符映射表中的位置，根据读取的位置信息在第 r 页字符映射表中查找每个字符 m 的原文。

[0038] 实施例 1

[0039] 下面描述根据本发明实施例 1 的数据加密方法。字符映射表的长度为 256。

[0040] 首先，随机生成字符映射表，字符映射表有 256 页，每页内容为所有 256 个 ASCII 字符（即，字符映射表的每一页中所有 256 个 ASCII 字符均只出现一次），记为 Dict1[256][256]。

[0041] 更详细地讲，可按照下面的方式生成字符映射表的每一页：(1) 设置数组 P[256] 的初始内容（例如，数组 P[256] 的初始内容可以是标准 ASCII 字符表的内容）；(2) 任取两个随机数 R1 和 R2，(0 ≤ R1 ≤ 255，0 ≤ R2 ≤ 255)；将 P[R1] 与 P[R2] 交换；(3) 重复执行操作 (2)，循环 N 次（例如，N ≥ 128)。

[0042] 这样生成的字符映射表的内容是随机的。可将生成的字符映射表以配置文件的形式，通过磁盘等介质复制并存储在各个通信节点的存储器中。

[0043] 通信节点的通信应用程序启动时加载该字符映射表。

[0044] 通信节点 A 在发送信息 M 前，对信息 M 进行加密（编码），加密过程如下：对于信息 M 的每一个字符 m，可知 0 ≤ m 所对应的 ASCII 码的十进制值≤ 255，取一个随机数 r(0 ≤ r ≤ 255)。在字符映射表 Dict1 的第 r 页中查找字符 m 所在的位置 n，即 Dict1[r][n] = m。将字符 m 编码为 (r，n)，最后得到信息 M(M = m1m2m3m4…) 的编码形式如：r1，n1，r2，n2，r3，n3，r4，n4……。

[0045] 通信节点 B 收到密文信息 (M') 后解密（解码）过程如下：循环读取信息 M'，每次取两个字节，记第一个字节为 r，第二个字节为 n。查找 Dict1[r][n] 得到字符 m，即 m = Dict1[r][n]。当循环结束时，把所有解得的字符依次连接起来即得到原文 M。

[0046] 这种方法的优点在于，对于相同的信息 M，每次加密的结果都可能相同，也可能不同，还可能部分相同，加密是完全随机的，不能利用差分和线性方法攻击，破解难度趋于无穷大。

[0047] 实施例 2

[0048] 在根据本发明实施例 1 的加密方法中，信息的每一个字符被编码为 2 个字节，使加密后的信息长度增加了一倍，根据本发明实施例 2 的数据加密方法进行了如下改进：

[0049] 字符映射表只有 1 页，内容为所有 256 个 ASCII 字符，每个 ASCII 码字符在字符映射表中只出现一次，字符映射表记为 Dict2[256]，按照实施例 1 中生成一页字符映射表的内容的方法来生成随机的 1 页字符映射表的内容。由于一页字符映射表内容比较少，因此可将该字符映射表作为源程序编译到通信程序里，完成字符映射表的分发。

[0050] 通信节点 A 在发送信息 M 前，对信息 M 进行编码，编码过程如下：

[0051] 对于信息 M 的每一个字符 m，在字符映射表 Dict2[256] 中查找字符 m 所在的位置 n，即，Dict2[n] = m。将字符 m 编码为 n，最后得到信息 M(M = m1m2m3m4…) 的编码形式如：n1，n2，n3，n4……。

[0052] 通信节点 B 收到密文信息 (M') 后解密过程如下：循环读取信息 M'，每次取一个字节，记为 n。查找 Dict2[n] 得到字符 m，即，m = Dict2[n]。当循环结束时，把所有解密得到的字符依次连接起来即得到信息原文 M。

[0053] 这种方法的优点在于加密信息长度没有增加，并且加密强度并没有减小。

[0054] 实施例 3

[0055] 图 3 和图 4 分别示出了根据本发明实施例 3 的数据加密方法的加密流程和解密流程。

[0056] 在根据本发明的实施例 2 的加密方法中，虽然信息编码没有变长，但是在解码时需要在解密字符映射表查找字符 m 的位置，解码速度不够快，根据本发明实施例 3 的数据加密方法进行了如下改进。

[0057] 字符映射表的内容及生成方式与实施例 2 一致，字符映射表的分发方式也与实施例 2 一致，字符映射表记为 Dict3_enc[256]。

[0058] 通信节点 A 在发送信息 M 之前，对信息 M 进行编码，编码过程如下：对于信息 M 的每一个字符 m，将字符 m 直接映射为字符映射表中的字符 n，即 n = Dict3_enc[m]，将字符 m 编码为 n。具体地讲，对于将被发送的信息 M 中的每个字符 m，字符 m 所对应的 ASCII 码的十进制值为 x(字符 m 所对应的 ASCII 码是唯一且固定的，并且 0 ≤ x ≤ 255)，字符映射表中第 x 个字符为 n，将字符 m 映射为字符 n，作为所述字符 m 的加密密文。最后得到信息 M(M = m1m2m3m4…) 的编码形式如：n1，n2，n3，n4……。

[0059] 通信节点 B 收到密文信息 (M') 后解密过程如下：首先构造解密字符映射表 Dict3_dec[256]，构造方式为：Dict3_dec[Dict3_enc[i]] = i(0 ≤ i ≤ 255)。

[0060] 具体地讲，对于字符映射表 Dict3_enc[256] 中的每一个字符 a，其所对应的 ASCII 码的十进制值为 y，字符映射表中第 y 个字符为 b，将字符 b 布置在解密字符映射表 Dict3_dec[256] 的第 y 个位置，由此构造解密字符映射表。

[0061] 在解密时，循环读取信息 M'，每次取一个字符，记为 n。将 n 直接映射为 m，即 m = Dict3_dec[n]。具体地，获得 n 在加密字符映射表中的位置 x(即，n 位于解密字符映射表的第 x 个位置)，x 值所对应的 ASCII 码字符为 m，由此将 n 直接映射为 m，作为解密的原文 (即，将 x 值所对应的 ASCII 码字符 m 作为解密的原文)。

[0062] 当循环结束时，将所有解密得到的字符依次连接起来即得到信息原文 M。

[0063] 这种方法的优点在于加密信息长度没有增加，并且加密强度并没有减小，而且加密的速度和解密的速度一样都非常快。

[0064] 实施例 4

[0065] 实施例 3 的加密方法在加密 / 解密速度、强度等方便都很优良，但是将字符映射表的内容编译到程序里的做法安全性可能不足。如果攻击者获得了程序执行文件，可以通过反编译的办法获得加密算法和字符映射表内容。在根据本发明的实施例 4 中，可以改进字符映射表及加密算法的存储方式。可以将字符映射表和 / 或加密解密算法代码存储在一个安全模块 (Secure Access Module，SAM) 中，使安全模块成为各个通信节点的一个设备，通

信节点需要数据加密和解密时均通过该安全模块进行。

[0066] 安全模块之所以安全是因为它能够有效防止大多数的破解方法，除了软件算法本身保证安全外，安全模块的硬件也具有一定的安全特性，一般地包括但不限于以下方法：(1) 具有电压检测模块对抗高低电压攻击；(2) 具有频率检测模块对抗高低频率攻击；(3) 具有多种检测传感器，例如高压和低压传感器、频率传感器、滤波器、脉冲传感器、温度传感器等，具有传感器寿命测试功能，一旦安全模块检测到非法探测，将启动内部的数据自毁功能，将所存储数据全部清除；(4) 具有总线加密功能，具有金属屏蔽防护层，在检测到外部攻击后内部数据自毁。因此，即使安全模块被攻击者获得，也不能获得字符映射表内容和加密算法，这样就大大增加了系统的安全性。

[0067] 实施例 5

[0068] 图 5 示出了根据本发明实施例 5 的数据加密方法的总体框图。在前面的四种实施例中，加密 / 解密算法均只用到了两个参数：字符映射表和信息，使用时间长了以后字符映射表内容也可能会被猜到。因此，在根据本发明的实施例 5 中，可增加一个分散因子 Div 参与计算，在每次数据加密 / 解密之前用分散因子与相应使用的字符映射表做一次分散运算得到一个新的字符映射表，用这个新的字符映射表作为加密 / 解密的基础。此时，加密算法改为 Enc(Dict,Div,M)，解密算法改为 Dec(Dict,Div,M')。分散因子与字符映射表的分散运算的算法可以用非常简单算法避免增加计算强度。

[0069] 通过使用分散因子，可以达到每次加密所用的字符映射表都不一样，进一步增加了破解的难度。

[0070] 上述加密方法中的对信息的加密仅仅是用字符映射表对信息进行映射，解密也只是将信息进行反映射，其计算效率是非常高的，几乎可以忽略不计。但是由于字符映射表的内容是随机的，字符映射表长度大于或等于 256，内容覆盖所有的 256 个 ASCII 字符，该字符映射表的内容至少有 256 的阶乘 (即，256 ！ ＝ 8.57e+506) 种组合。由于加密的过程不涉及具体的数学算法，无法通过数学求解的方式进行解密，决定了在这种情况下即使算法是公开的也只能使用穷举法暴力破解，没有其它捷径。在只有密文信息的情况下想通过暴力的办法还原出信息原文或者加密用的字符映射表，在现有技术水平条件下进行破解非常困难。

[0071] 以上的实施方式提到了不同的字符映射表生成方法和不同的加密方法，但是这些方法仅仅是示例性的，实际上远远不止这几种方法。

[0072] 虽然本发明是参照其示例性的实施例被具体描述和显示的，但是本领域的普通技术人员应该理解，在不脱离由权利要求限定的本发明的精神和范围的情况下，可以对其进行形式和细节的各种改变。

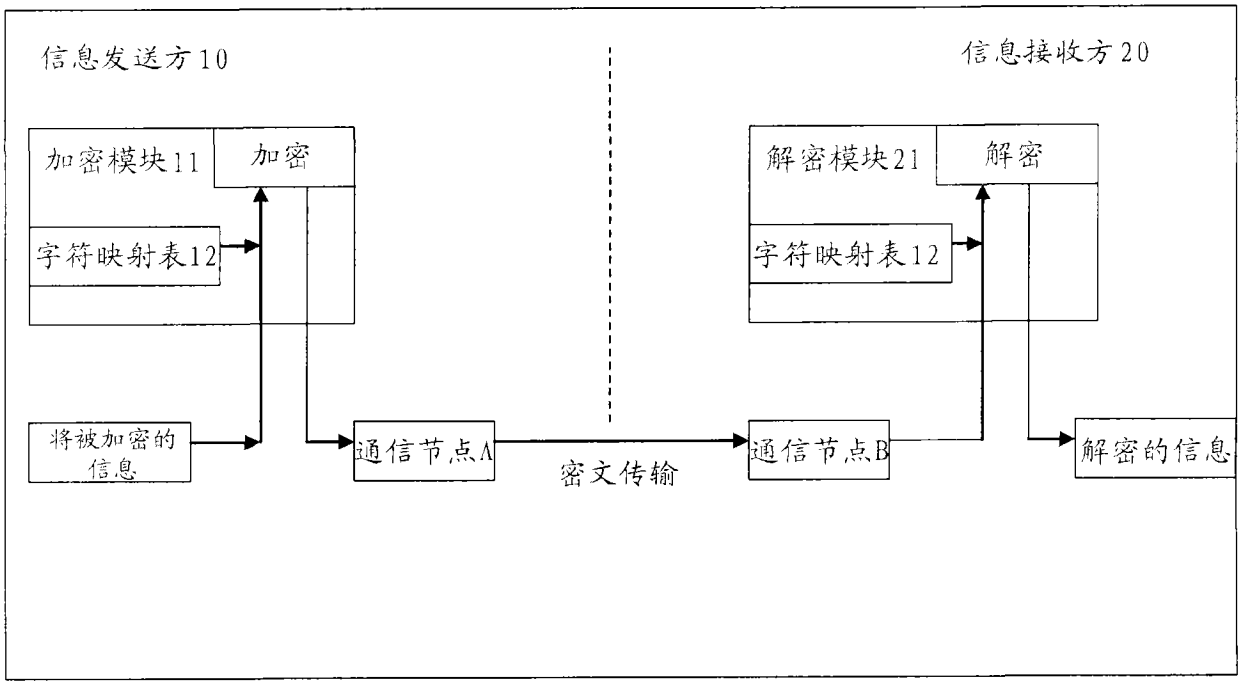

信息发送方10
信息接收方20
加密模块11
加密
字符映射表12
解密模块21
解密
字符映射表12
将被加密的信息
通信节点A
密文传输
通信节点B
解密的信息

图 1

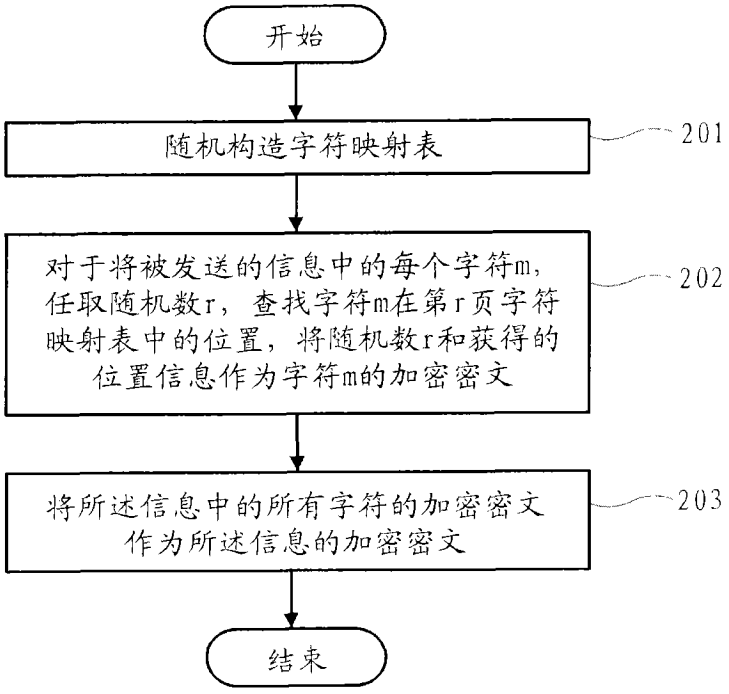

开始
随机构造字符映射表
201
对于将被发送的信息中的每个字符m，任取随机数r，查找字符m在第r页字符映射表中的位置，将随机数r和获得的位置信息作为字符m的加密密文
202
将所述信息中的所有字符的加密密文作为所述信息的加密密文
203
结束

图 2

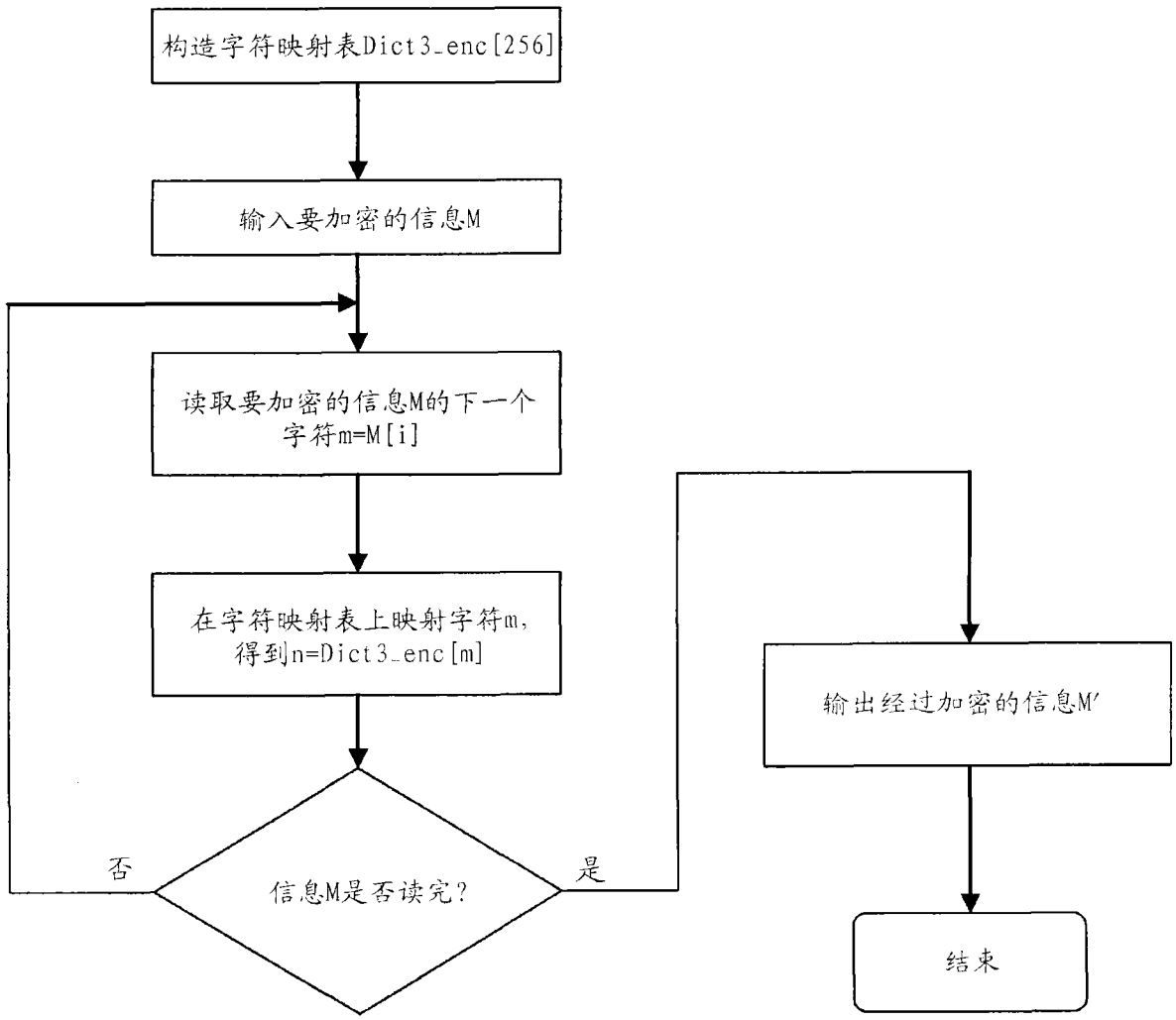

构造字符映射表Dict3_enc[256]
输入要加密的信息M
读取要加密的信息M的下一个字符m=M[i]
在字符映射表上映射字符m，得到n=Dict3_enc[m]
信息M是否读完？
否
是
输出经过加密的信息M′
结束

图 3

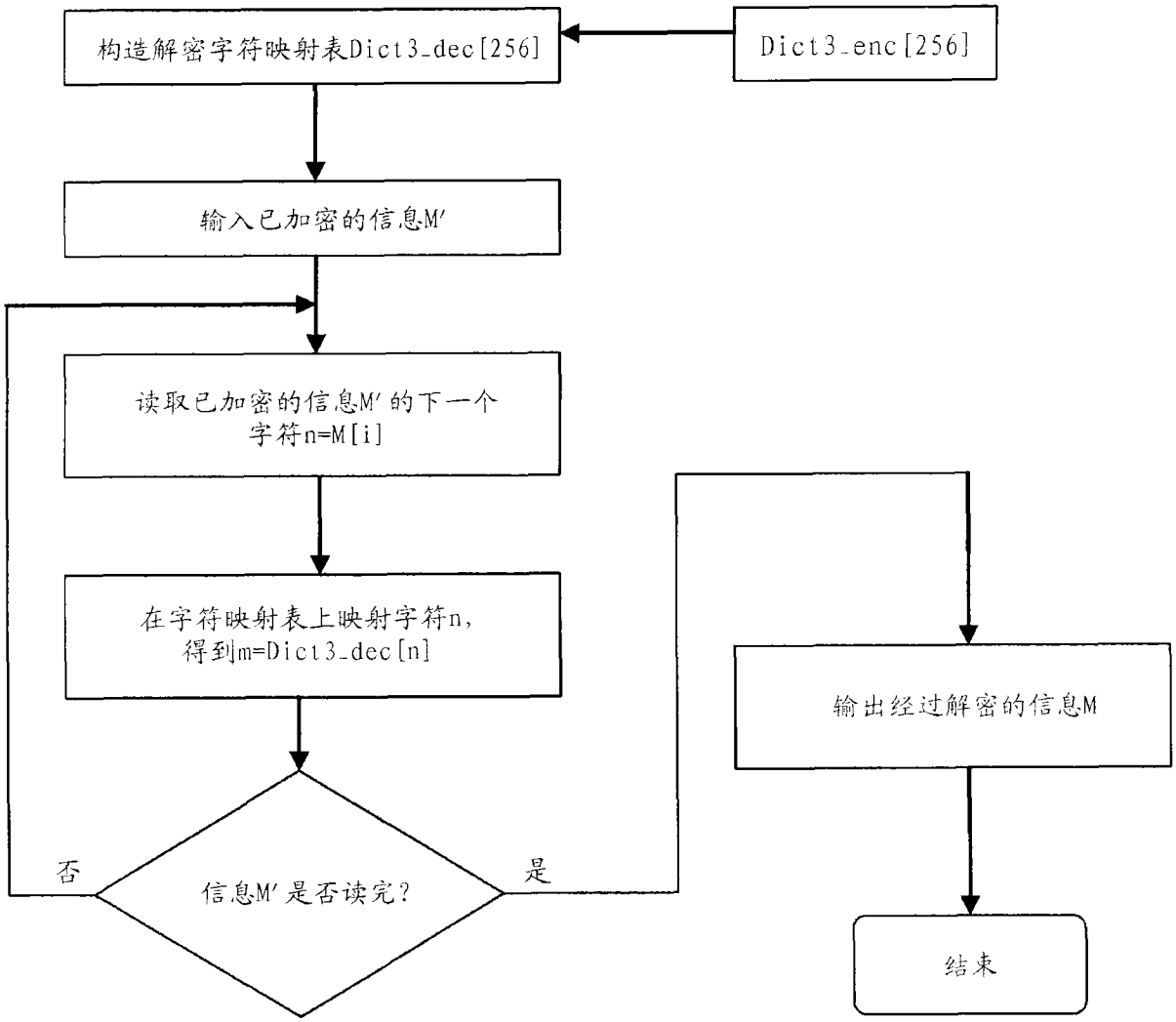

构造解密字符映射表Dict3_dec[256]
Dict3_enc[256]
输入已加密的信息M′
读取已加密的信息M′的下一个字符n=M[i]
在字符映射表上映射字符n，得到m=Dict3_dec[n]
信息M′是否读完？
否
是
输出经过解密的信息M
结束

图 4

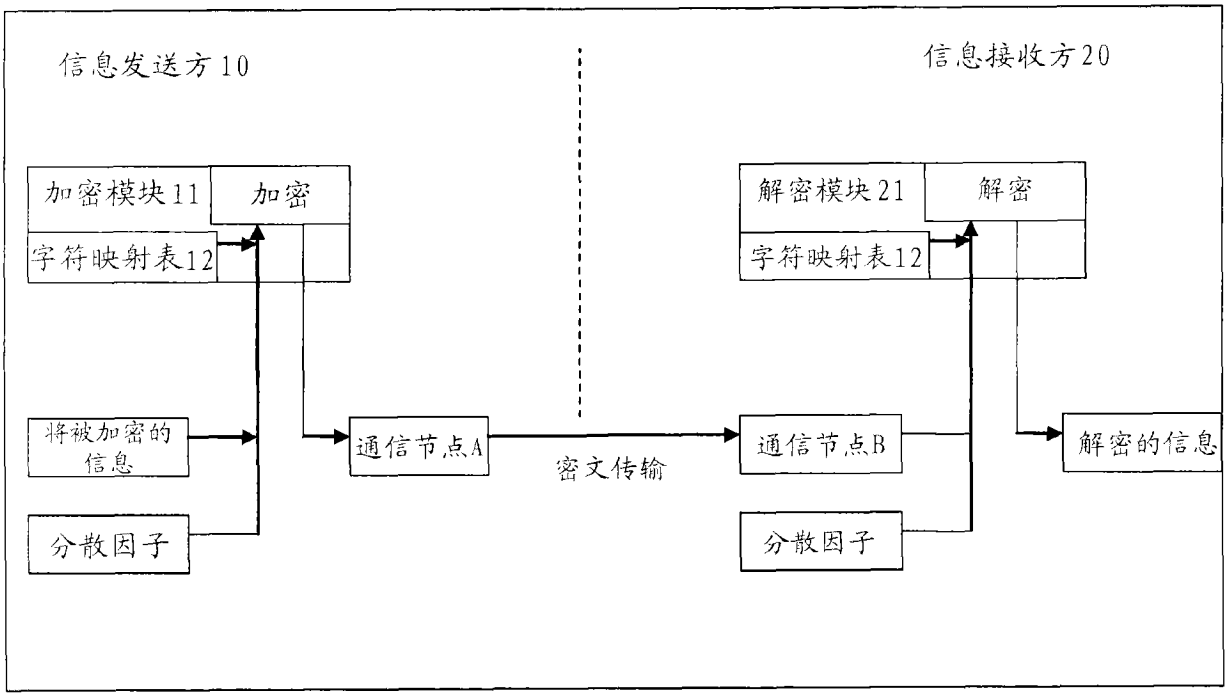

信息发送方10
信息接收方20
加密模块11
加密
字符映射表12
将被加密的信息
分散因子
通信节点A
密文传输
通信节点B
解密模块21
解密
字符映射表12
分散因子
解密的信息

图 5