(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 3 月 27 日 (27.03.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/044137 A1

(51) 国际专利分类号:
H04L 9/28 (2006.01)

(21) 国际申请号: PCT/CN2013/083291

(22) 国际申请日: 2013 年 9 月 11 日 (11.09.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210358087.0 2012 年 9 月 24 日 (24.09.2012) CN

(71) 申请人: **腾讯科技（深圳）有限公司** (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。

(72) 发明人: **陈恕胜** (CHEN, Shusheng); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。 **张坤** (ZHANG, Kun); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。 **熊正祥** (XIONG, Zhengxiang); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。 **刘莹雪** (LIU, Yingxue); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。 **臧悦** (ZANG, Yue); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。

(74) 代理人: **北京德琦知识产权代理有限公司** (DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路 1 号学院国际大厦 7 层, Beijing 100083 (CN)。

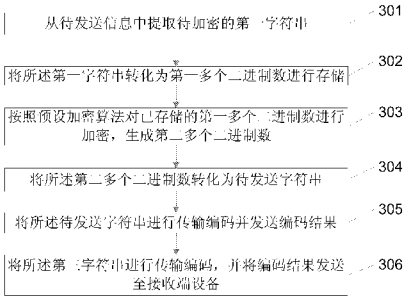
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) **Title**: COMMUNICATION ENCRYPTION AND DECRYPTION METHOD, DEVICE AND SYSTEM

(54) **发明名称** : 通信的加密和解密的方法、装置及系统

图 3 / **Fig. 3**



301 EXTRACTING A TO-BE-ENCRYPTED FIRST CHARACTER STRING FROM THE TO-BE-TRANSMITTED INFORMATION
302 CONVERTING THE FIRST CHARACTER STRING INTO A PLURALITY OF FIRST BINARY NUMBERS FOR STORAGE
303 ENCRYPTING THE STORED PLURALITY OF FIRST BINARY NUMBERS ACCORDING TO A PRESET ENCRYPTION ALGORITHM TO GENERATE A PLURALITY OF SECOND BINARY NUMBERS
304 CONVERTING THE PLURALITY OF SECOND BINARY NUMBERS INTO A TO-BE-TRANSMITTED CHARACTER STRING
305 CONDUCTING TRANSMISSION ENCODING ON THE TO-BE-TRANSMITTED CHARACTER STRING, AND TRANSMITTING THE ENCODING RESULT
306 CONDUCTING TRANSMISSION ENCODING ON THE THIRD CHARACTER STRING, AND TRANSMITTING THE ENCODING RESULT TO A RECEIVING TERMINAL DEVICE

(57) **Abstract**: Disclosed are a communication encryption and decryption method, device and system. The encryption process comprises: extracting a to-be-encrypted first character string from the to-be-transmitted information; converting the first character string into a plurality of first binary numbers for storage; encrypting the stored plurality of first binary numbers according to a preset encryption algorithm to generate a plurality of second binary numbers; converting the plurality of second binary numbers into a to-be-transmitted character string; conducting transmission encoding on the to-be-transmitted character string, and transmitting the encoding result. The decryption process comprises: receiving the to-be-processed information transmitted by a transmitting terminal; conducting transmission decoding on the to-be-processed information to obtain a third character string; converting the third character string into a plurality of third binary numbers for storage; decrypting the stored plurality of third binary numbers according to a preset decryption algorithm to generate a plurality of fourth binary numbers; and converting the plurality of fourth binary numbers into a fourth character string.

(57) **摘要**:

[见续页]

WO 2014/044137 A1

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种通信的加密和解密的方法、装置及系统。加密流程包括：从待发送信息中提取待加密的第一字符串；将所述第一字符串转化为第一多个二进制数进行存储；按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数；将所述第二多个二进制数转化为待发送字符串；将所述待发送字符串进行传输编码并发送编码结果。解密流程包括：接收发送端发送的待处理信息；将所述待处理信息进行传输解码，得到第三字符串；将所述第三字符串转化为第三多个二进制数进行存储；按照预设解密算法对已存储的第三多个二进制数进行解密，生成第四多个二进制数；将所述第四多个二进制数转化为第四字符串。

通信的加密和解密的方法、装置及系统

技术领域

本发明涉及信息处理领域，尤其涉及一种通信的加密和解密的方法、装置及系统。

发明背景

为了用户信息的安全，必须要对用户使用的客户端与服务端之间的通信信息进行全程加密，以防止用户信息泄漏。目前常用的加密算法有TEA、BASE64、MD5等。

发明内容

一种通信的加密的方法，包括:

从待发送信息中提取待加密的第一字符串;

将所述第一字符串转化为第一多个二进制数进行存储;

按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数;

将所述第二多个二进制数转化为待发送字符串;

将所述待发送字符串进行传输编码并发送编码结果。

一种通信的解密的方法，其特征在于，包括:

接收发送端发送的待处理信息;

将所述待处理信息进行传输解码，得到第一字符串;

将所述第一字符串转化为第一多个二进制数进行存储;

按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数;

将所述第二多个二进制数转化为第二字符串。

一种通信的加密的装置，其特征在于，包括:

提取单元，用于从待发送信息中提取待加密的第一字符串;

转化单元，用于将所述提取单元得到的第一字符串转化为第一多个二进制数进行存储;

加密单元，用于按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数;

所述转化单元，还用于将所述第二多个二进制数转化为待发送字符串;

编码单元，用于将所述转化单元生成的待发送字符串进行传输编码;

发送单元，用于发送所述编码单元生成的编码结果。

一种通信的解密的装置，其特征在于，包括:

接收单元，用于接收发送端发送的待处理信息;

解码单元，用于将所述接收单元接收的待处理信息进行传输解码，得到第一字符串;

转化单元，用于将所述第一字符串转化为第一多个二进制数进行存储;

解密单元，用于按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数;

所述转化单元，还用于将所述第二多个二进制数转化为第二字符串。

一种通信的加密和解密的系统，包括上述通信的加密的装置和上述通信的解密的装置。

本发明实施例提供了一种通信的加密和解密的方法、装置及系统，通过将待发送信息转化为二进制数进行存储，然后对存储信息进行加密或解密处理，再将加密结果或解密结果导出并转化为字符串使用，从而

实现加密和解密的流程。

附图简要说明

图 1 为本发明实施例提供的一种通信系统示意图;

图 2 为本发明实施例提供的一种计算设备结构图;

图 3 为本发明实施例提供的一种通信的加密的方法流程图;

图 4 为本发明实施例提供的另一种通信的加密的方法流程图;

图 5 为本发明实施例提供的另一种通信的加密的系统的组成框图;

图 6 为本发明实施例提供的一种通信的解密的方法流程图;

图 7 为本发明实施例提供的另一种通信的解密的方法流程图;

图 8 为本发明实施例提供的另一种通信的解密的方法流程图;

图 9 为本发明实施例提供的一种通信的加密的装置的组成框图;

图 10 为本发明实施例提供的另一种通信的加密的装置的组成框图;

图 11 为本发明实施例提供的另一种通信的加密的装置的组成框图;

图 12 为本发明实施例提供的一种通信的解密的装置的组成框图;

图 13 为本发明实施例提供的另一种通信的解密的装置的组成框图;

图 14 为本发明实施例提供的另一种通信的解密的装置的组成框图;

图 15 为本发明实施例提供的一种通信的加密和解密的系统的组成框图。

实施本发明的方式

为了描述上的简洁和直观，下文通过描述若干代表性的实施例来对本发明的方案进行阐述。实施例中大量的细节仅用于帮助理解本发明的方案。但是很明显，本发明的技术方案实现时可以不局限于这些细节。为了避免不必要地模糊了本发明的方案，一些实施方式没有进行细致地

描述，而是仅给出了框架。下文中，“包括”是指“包括但不限于”，“根据……”是指“至少根据……，但不限于仅根据……”。由于汉语的语言习惯，下文中没有特别指出一个成分的数量时，意味着该成分可以是一个也可以是多个，或可理解为至少一个。

图 1 为一个实施例的通信系统的示意图。如图 1 所示，通信系统包括服务器设备 10，通信网络 20 和用户终端设备。用户终端设备可以是个人电脑 30、手机 40、平板电脑 50，还可以是其它各种移动互联网终端（MID），如可以利用各种无线通信技术连接到互联网的电子阅读器、掌上游戏终端等。上述服务器设备和用户终端设备均可以应用本发明实施例的加密、解密方法。后文将实现加密、解密方法的装置统称为计算设备或计算机。当应用加密方法的计算设备是服务器时，应用解密方法对服务器的加密信息进行解密的计算设备可以是用户终端，反之亦然。

图 2 是一个实施例的计算设备的结构示意图。如图 2 所示，计算机 200 可以是能够实现本发明实施例提供的方法和软件系统的计算设备。例如，计算机 200 可以是个人电脑或便携设备，例如笔记本电脑、平板电脑、手机或智能手机，等。计算机 200 还可以是与上述设备通过网络相连的服务器。

计算机 200 可以具有不同的性能和特征。各种可能的实现方式都在本文的保护范围内。例如，计算机 200 可以包括按键区/键盘 256，还可以包括一个显示器 254，如液晶显示器（LCD），或者具有高级功能的显示器，例如触摸感应 2D 或 3D 显示器。一个例子中，一个具有 web 功能的计算机 200 可以包括一个或多个物理键盘或虚拟键盘，以及大容量存储装置 230。

计算机 200 也可以包括或允许各种操作系统 241，例如 WindowsTM 或 LinuxTM 操作系统，或移动操作系统，如 iOSTM，AndroidTM，或

Windows MobileTM 等。计算机 200 可以包括或运行各种应用程序 242，例如通信加/解密应用 245。应用程序 242 能够通过网络与其它设备进行加密通信。

此外，计算机 200 可以包括一个或多个处理器可读的非易失性存储介质 230 和一个或多个与存储介质 230 通信的处理器 222。例如，处理器可读的非易失性存储介质 230 可以是 RAM、闪存、ROM、EPROM、EEPROM、寄存器、硬盘、移动硬盘、CD-ROM，或其它各种形式的非易失性存储介质。存储介质 230 可以存储一系列指令或包含指令的单元和/或模块，用于完成本发明各种实施例的操作。处理器可以执行上述指令，完成各种实施例中的操作。

本发明实施例提供了一种通信的加密的方法，可以应用于基于 WEB 通信的计算设备，例如，手机、平板电脑等客户端设备，和运营商或业务提供商的服务器等服务端设备。

在本发明实施例中，通信双方的计算设备，如客户端设备和服务端设备，需要分别设置至少一加密模块和至少一解密模块或通信加/解密应用程序。通信加/解密应用程序可以利用 Javascript 实现。

图 3 为本发明实施例提供的一种通信的加密方法。该方法为加密模块侧的方法，可以包括以下步骤。

301、从待发送信息中提取待加密的第一字符串。

其中，所述待发送信息为由客户端设备发送至服务端设备的信息，可以包括如用户名和密码等用于登录业务的用户信息，也可以包括某项 WEB 业务的数据信息，这些信息可以是加密过的信息，也可以是未加密的信息，本发明实施例对此不进行限制。

在 WEB 服务中，待发送信息可以以 JSON（JavaScript Object Notation）形式进行存放，例如，[object Object] :{"nick":"自选股"}。故

从待发送信息中可直接提取第一字符串{"nick":"自选股"} 。

302、将所述第一字符串转化为第一多个二进制数进行存储。

一个实施例中，将所述第一字符串转化为第一多个二进制数进行存储的具体实现方法可以如图 4 所示。该方法可以包括以下步骤。

3021、将所述待加密的第一字符串转化为第二字符串。

一个实施例中，所述第二字符串中的每个字符对应一个字节。

在 WEB 服务中，信息以字符串形式进行存放，可能会包含英文字母、英文符号、中文汉字、中文符号等信息，而单个中文字符大多为多字节字符。例如，单个中文字符对应的编码数值需要占用超过一个字节的存储空间。

步骤 3021 的转化目的在于将对应的编码数值需要占用超过一个字节的存储空间的字符转化为若干个对应的编码数值只占用一个字节的存储空间的字符，以便后续加密处理。

例如，在 Javascript 中，第一字符串可以以 Unicode 编码存放，可使用 UTF-8 编码方式将第一字符串转化为第二字符串。例如，第一字符串为"nick":"自选股"，则对应的第二字符串为"nick":"è‡ªé€‰è‚¡"。上述编码方式仅仅是例子，其它实施例可以采用其它可行的编码方式，这里不做限定。

3022、将所述第二字符串转化为第一字符数组。

其中，所述第一字符数组中的一个元素对应第二字符串中的一个字符的单字节编码数值。

在本实施例中，由于在步骤 303 之前执行了步骤 302，在步骤 303 中，直接确定每个字符对应的编码数值即可。

例如，将所述第二字符串转化为第一字符数组可以遵循 ACSII 码表，例如，第二字符串为"nick":"è‡ªé€‰è‚¡"，则对应的第一字符数组为[123,

34, 110, 105, 99, 107, 34, 58, 34, 232, 135, 170, 233, 128, 137, 232, 130, 161, 34, 125]。

3023、按照预设值，将所述第一字符数组内的元素分割成若干个数组块。

其中，每个数组块包括预设数量个元素。

其中，预设值为自然数，可根据实际需要进行设定，可以将字符数组内的所有元素按照预设数量进行分块处理，每个数组块具有预设数量个元素。

以预设数量为 4 为例，则将所述字符数组内的元素分割成若干个数组块具体可以包括：按照所述第一字符数组内的元素排列顺序，依次将相邻的 4 个元素划分为一个数组块。

3024、将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储。

以预设数量为 4 为例，将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储可以包括：

将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数。将所述每个数组块对应的一个 32 位二进制数进行存储。

303、按照预设的加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数。

其中，预设加密算法可以包括 TEA、MD5 等目前 WEB 服务中常用的加密算法。在各实施例中，不同业务类型待发送信息的使用的加密算法也可以不同。

304、将所述第二多个二进制数转化为待发送字符串。

图 5 为所述将所述第二多个二进制数转化为待发送字符串的方法。

该方法可以包括以下步骤。

3041、将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

例如，在本实施例中，若在步骤 3021 中的第一字符数组为[123, 34, 110, 105, 99, 107, 34, 58, 34, 232, 135, 170, 233, 128, 137, 232, 130, 161, 34, 125]，则经过步骤 3041 可得到对应的第二字符数组为[234, 109, 33, 119, 105, 146, 35, 0, 147, 240, 52, 189, 187, 172, 109, 20, 182, 48, 131, 71, 255, 98, 83, 140, 113, 228, 59, 246, 232, 150, 55, 180]。

3042、将第二字符数组转化为待发送字符串。

其中，所述第二字符数组中的一个元素对应待发送字符串中的一个字符的单字节编码数值。

其中，所述第二字符数组中的一个元素对应待发送字符串中的一个字符的单字节编码数值。

其中，所述将第二字符数组转化为待发送字符串可以遵循 ACSII 码表。

例如，在本实施例中，若第二字符数组为[234, 109, 33, 119, 105, 146, 35,0,147,240,52,189,187,172,109,20,182,48,131,71,255,98,83,140,113,228, 59,246,232,150,55,180]，则其对应的待发送字符串为“ê m!wi’ #”。

305、将所述待发送字符串进行传输编码并发送编码结果。

为方便 HTTP 或 HTTPs 的传输方式，在本实施例中通过步骤 305 将所述待发送字符串进行传输编码。

在本实施例中，将所述待发送字符串进行传输编码可遵循 BASE64 编码方式，例如，若待发送三字符串为“ê m!wi’ #”，则对应的编码结果为 6m0hd2mSIwCT8DS9u6xtFLYwg0f/YlOMceQ79uiWN7Q=。

图 6 为本发明实施例的一种通信的解密的方法。该方法为解密模块

侧的方法，可以包括以下步骤。

601、接收发送端发送的待处理信息。

其中，所述待处理信息即为加密模块发送过来的加密信息。

602、将所述待处理信息进行传输解码，得到第一字符串。

将所述待处理信息进行传输解码，得到第一字符串需要遵循加密模块使用的传输编码方式。加密模块和解密模块这两侧之间使用的各类加解密算法和编解码方式可以原先匹配好，也可以及时通信告知，本发明实施例对此不进行限制。

以 BASE63 编码方式为例，若所述待处理信息为 6m0hd2mSIwCT8DS9u6xtFLYwg0f/YlOMceQ79uiWN7Q=，则对应的第一字符串为“ê m!wi’ #”。

603、将所述第一字符串转化为第一多个二进制数进行存储。

图 7 为所述将所述第一字符串转化为第一多个二进制数进行存储的实现方法。该方法可以包括以下步骤。

6031、将所述待解密的第一字符串转化为第一字符数组。

其中，所述第一字符数组中的一个元素对应第三字符串中的一个字符的单字节编码数值。

例如，将所述第一字符串转化为第一字符数组可遵循 ACSII 码表，若第一字符串为“ê m!wi’ #”，则对应的第二字符数组为[234, 109, 33, 119, 105, 146, 35, 0, 147, 240, 52, 189, 187, 172, 109, 20, 182, 48, 131, 71, 255, 98, 83, 140, 113, 228, 59, 246, 232, 150, 55, 180]。

6032、按照预设值，将所述字符数组内的元素分割成若干个数组块。

一个实施例中，每个数组块包括预设数量的元素。

预设数量可以与加密模块的设置相同。

例如，预设数量为 4 时，将所述字符数组内的元素分割成若干个数

组块具体可以包括：按照所述第一字符数组内的元素排列顺序，依次将相邻的 4 个元素划分为一个数组块。

6033、将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储。

例如，预设数量为 4，则将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储可以包括:

将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数。将所述每个数组块对应的一个 32 位二进制数进行存储。

604、按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数。

其中，预设解密算法应与加密模块侧设置的加密算法相对应。

605、将所述第二多个二进制数转化为第二字符串。

图 8 为将所述第二多个二进制数转化为第二字符串的方法。该方法可以包括以下步骤。

6051、将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

例如，若在步骤 3031 中的第一字符数组为[234, 109, 33, 119, 105, 146, 35, 0, 147, 240, 52, 189, 187, 172, 109, 20, 182, 48, 131, 71, 255, 98, 83, 140, 113, 228, 59, 246, 232, 150, 55, 180]，则经过步骤 6051 可得到对应的第二字符数组为[123, 34, 110, 105,99,107, 34, 58, 34, 232, 135, 170, 233, 128, 137,232,130,161,34,125]。

6052、将第二字符数组转化为第二字符串。

其中，所述第二字符数组中的一个元素对应所述第二字符串中的一个字符的单字节编码数值。

一个实施例中，将所述第二字符数组转化为第二字符串可以遵循ACSII码表，例如，若第二字符数组为[123, 34, 110, 105, 99, 107, 34, 58, 34, 232, 135, 170, 233, 128,137,232,130,161,34,125]，则第二字符串为"nick":"è‡ªé€‰è‚¡"。

606、将所述第二字符串转化为所述待处理信息的源信息。

一个实施例中，可以将每个字符对应一个字节的第二字符串转化为Unicode编码进行存放。步骤606的转化方法可以遵循UTF-8编码。例如，若第二字符串为"nick":"è‡ªé€‰è‚¡"，则对应的所述待处理信息对应的源信息为"nick":"自选股"，并可以将"nick":"自选股"以JSON形式存储起来。

以上加密和解密方法中所使用的字符编码方式可以是任意合适的编码方法，上面例子中使用的编码方式仅是示例，可以替换为其它编码方式。

本发明实施例提供了一种通信的加密和解密的方法，通过将待发送信息转化为二进制数进行存储，然后对存储信息进行加密或解密处理，再将加密结果或解密结果导出并转化为字符串使用，从而实现加密和解密的流程。本发明实施例通过对将待发送信息转化为二进制数进行存储，为加密算法提供了二进制格式的信息，使得各种加密算法也可以使用在Javascript语言环境中。根据WEB服务的具体需要，使用不同的加密算法，保证了在javascript环境下用户信息的安全。

图9为本发明实施例提供的一种通信的加密的装置90。该装置可以包括：提取单元91、转化单元92、加密单元93、编码单元94、发送单元95。

提取单元91，用于从待发送信息中提取待加密的第一字符串。

转化单元92，用于将所述提取单元91得到的第一字符串转化为第

一多个二进制数进行存储。

加密单元 93，用于按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数。

所述转化单元 92，还用于将所述第二多个二进制数转化为待发送字符串。

编码单元 94，用于将所述转化单元 92 生成的待发送字符串进行传输编码。

发送单元 95，用于发送所述编码单元生成的编码结果。

一个实施例中，如图 10 所示，所述转化单元 92 可以包括：第一转化模块 921、第二转化模块 922、分割模块 923、第三转化模块 924、存储模块 925。

第一转化模块 921，用于将所述待加密第一字符串转化为第二字符串；其中，所述第二字符串中的每个字符对应一个字节。

第二转化模块 922，用于将所述第一转化模块 921 得到的第二字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第二字符串中的一个字符的单字节编码数值。

分割模块 923，用于将所述第二转化模块 922 得到的字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设数量的元素。

第三转化模块 924，用于将分割模块 923 得到每个数组块中的元素分别转化成 8 位二进制数。

存储模块 925，用于将第三转化模块 923 得到的每个数组块对应的多个 8 位二进制数进行存储。

例如，预设数量为 4 时，所述分割模块 92 可以按照所述第一字符数组内的元素排列顺序，依次将相邻的 4 个元素划分为一个数组块。

所述第三转化模块 794，用于将每个数组块内的 4 个元素分别转化

为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数。

所述存储模块 925，用于将所述每个数组块对应的一个 32 位二进制数进行存储。

一个实施例中，如图 11 所示，所述转化单元 92 包括：第四转化模块 926、第五转化模块 927。

第四转化模块 926，用于将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

第五转化模块 927，用于将所述第四转化模块 926 得到的第二字符数组转化为待发送字符串；其中，所述第二字符数组中的一个元素对应待发送字符串中的一个字符的单字节编码数值。

图 12 为本发明实施例提供的一种通信的解密的装置 120。该装置 120 可以包括：

接收单元 1201，用于接收发送端发送的待处理信息；

解码单元 1202，用于将所述接收单元 1201 接收的待处理信息进行传输解码，得到第一字符串；

转化单元 1203，用于将所述第一字符串转化为第一多个二进制数进行存储；

解密单元 1204，用于按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数；

所述转化单元 1203，还用于将所述第二多个二进制数转化为第二字符串。

一个实施例中，如图 13 所示，所述转化单元 1203 可以包括：

第一转化模块 1231，用于将所述待解密的第一字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第三字符串中的一

个字符的单字节编码数值。

分割模块 1232，用于按照预设值，将所述第一转化模块得到的字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设值数量的元素。

第二转化模块 1233，用于将每个数组块中的元素分别转化成 8 位二进制数。

存储模块 1234，用于将每个数组块对应的多个 8 位二进制数进行存储。

一个实施例中，所述分割模块 1232 用于按照所述第一字符数组内的元素排列情况，依次将相邻的 4 个元素划分为一个数组块。

所述第二转化模块 1233，用于将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数。

所述存储模块 1234，用于将所述每个数组块对应的一个 32 位二进制数进行存储。

一个实施例中，如图 16 所示，所述转化单元 1203 包括：第三转化模块 1235、第四转化模块 1236。

第三转化模块 1235，用于将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

第四转化模块 1236，用于将所述第三转化模块 1235 得到的第二字符数组转化为第二字符串；其中，所述第二字符数组中的一个元素对应所述第二字符串中的一个字符的单字节编码数值。

图 14 为本发明实施例提供的一种通信的加密和解密的系统。该系统可以包括上述通信的加密的装置 90 和通信的解密的装置 120。

本发明实施例提供了一种通信的加密和解密的装置及系统，通过将

待发送信息转化为二进制数进行存储，然后对存储信息进行加密或解密处理，再将加密结果或解密结果导出并转化为字符串使用，从而实现加密和解密的流程。本发明实施例通过对将待发送信息转化为二进制数进行存储，为加密算法提供了二进制格式的信息，使得各种加密算法可以使用在 Javascript 语言环境中，保证了在 javascript 环境下用户信息的安全。

需要说明的是，上述各流程和各结构图中不是所有的步骤和模块都是必须的，可以根据实际的需要忽略某些步骤或模块。各步骤的执行顺序不是固定的，可以根据需要进行调整。各模块的划分仅仅是为了便于描述采用的功能上的划分，实际实现时，一个模块可以分由多个模块实现，多个模块的功能也可以由同一个模块实现，这些模块可以位于同一个设备中，也可以位于不同的设备中。另外，上面描述中采用“第一”、“第二”仅仅为了方便区分具有同一含义的两个对象，并不表示其有实质的区别。

各实施例中的硬件模块可以以机械方式或电子方式实现。例如，一个硬件模块可以包括专门设计的永久性电路或逻辑器件（如专用处理器，如 FPGA 或 ASIC）用于完成特定的操作。硬件模块也可以包括由软件临时配置的可编程逻辑器件或电路（如包括通用处理器或其它可编程处理器）用于执行特定操作。至于具体采用机械方式，或是采用专用的永久性电路，或是采用临时配置的电路（如由软件进行配置）来实现硬件模块，可以根据成本和时间上的考虑来决定。

本发明还提供了一种机器可读的存储介质，存储用于使一机器（可以是个人计算机，服务器，或者网络设备等）执行如本文所述方法的指令。具体地，可以提供配有存储介质的系统或者装置，在该存储介质上存储着实现上述实施例中任一实施例的功能的软件程序代码，且使该系

统或者装置的计算机（或 CPU 或 MPU）读出并执行存储在存储介质中的程序代码。此外，还可以通过基于程序代码的指令使计算机上操作的操作系统等来完成部分或者全部的实际操作。还可以将从存储介质读出的程序代码写到插入计算机内的扩展板中所设置的存储器中或者写到与计算机相连接的扩展单元中设置的存储器中，随后基于程序代码的指令使安装在扩展板或者扩展单元上的 CPU 等来执行部分和全部实际操作，从而实现上述实施例中任一实施例的功能。

用于提供程序代码的存储介质实施例包括软盘、硬盘、磁光盘、光盘（如 CD-ROM、CD-R、CD-RW、DVD-ROM、DVD-RAM、DVD-RW、DVD+RW）、磁带、非易失性存储卡和 ROM。可选择地，可以由通信网络从服务器计算机上下载程序代码。

综上所述，权利要求的范围不应局限于以上描述的例子中的实施方式，而应当将说明书作为一个整体并给予最宽泛的解释。

权利要求书

1、一种通信的加密的方法，其特征在于，包括:

从待发送信息中提取待加密的第一字符串;

将所述第一字符串转化为第一多个二进制数进行存储;

按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数;

将所述第二多个二进制数转化为待发送字符串;

将所述待发送字符串进行传输编码并发送编码结果。

2、根据权利要求 1 所述的方法，其特征在于，所述将所述待加密字符串转化为第一多个二进制数进行存储包括:

将所述待加密第一字符串转化为第二字符串；其中，所述第二字符串中的每个字符对应一个字节;

将所述第二字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第二字符串中的一个字符的单字节编码数值;

按照预设值，将所述字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设值数量的元素;

将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储。

3、根据权利要求 2 所述的方法，其特征在于，当所述预设值为 4 时，所述按照预设值，将所述第一字符数组内的元素各自对应的单字节编码数值分割成若干个数组块包括:

按照所述第一字符数组内的元素排列情况，依次将相邻的 4 个元素划分为一个数组块;

则将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组

块对应的多个 8 位二进制数进行存储包括:

将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数;

将所述每个数组块对应的一个 32 位二进制数进行存储。

4、根据权利要求 1 所述的方法，其特征在于，所述将所述第二多个二进制数转化为待发送字符串包括:

将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组;

将第二字符数组转化为待发送字符串；其中，所述第二字符数组中的一个元素对应待发送字符串中的一个字符的单字节编码数值。

5、一种通信的解密的方法，其特征在于，包括:

接收发送端发送的待处理信息;

将所述待处理信息进行传输解码，得到第一字符串;

将所述第一字符串转化为第一多个二进制数进行存储;

按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数;

将所述第二多个二进制数转化为第二字符串。

6、根据权利要求 5 所述的方法，其特征在于，所述将所述第一字符串转化为第一多个二进制数进行存储包括:

将所述待解密的第一字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第三字符串中的一个字符的单字节编码数值;

按照预设值，将所述字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设值数量的元素;

将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块

对应的多个 8 位二进制数进行存储。

7、根据权利要求 6 所述的方法，其特征在于，当所述预设值为 4 时，所述按照预设值，将所述第一字符数组内的元素分割成若干个数组块包括:

按照所述第一字符数组内的元素排列情况，依次将相邻的 4 个元素划分为一个数组块;

则将每个数组块中的元素分别转化成 8 位二进制数，并将每个数组块对应的多个 8 位二进制数进行存储包括:

将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数;

将所述每个数组块对应的一个 32 位二进制数进行存储。

8、根据权利要求 6 所述的方法，其特征在于，所述将所述第二多个二进制数转化为第二字符串包括:

将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

将第二字符数组转化为第二字符串；其中，所述第二字符数组中的一个元素对应所述第二字符串中的一个字符的单字节编码数值。

9、一种通信的加密的装置，其特征在于，包括:

提取单元，用于从待发送信息中提取待加密的第一字符串;

转化单元，用于将所述提取单元得到的第一字符串转化为第一多个二进制数进行存储;

加密单元，用于按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数;

所述转化单元，还用于将所述第二多个二进制数转化为待发送字符串;

编码单元，用于将所述转化单元生成的待发送字符串进行传输编码；

发送单元，用于发送所述编码单元生成的编码结果。

10、根据权利要求 9 所述的装置，其特征在于，所述转化单元包括：

第一转化模块，用于将所述待加密第一字符串转化为第二字符串；其中，所述第二字符串中的每个字符对应一个字节；

第二转化模块，用于将所述第一转化模块得到的第二字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第二字符串中的一个字符的单字节编码数值；

分割模块，用于按照预设值，将所述第二转化模块得到的字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设值数量的元素；

第三转化模块，用于将分割模块得到每个数组块中的元素分别转化成 8 位二进制数；

存储模块，用于将第三转化模块得到的每个数组块对应的多个 8 位二进制数进行存储。

11、根据权利要求 10 所述的方法，其特征在于，所述分割模块用于在所述预设值为 4 时，按照所述第一字符数组内的元素排列情况，依次将相邻的 4 个元素划分为一个数组块；

所述第三转化模块，用于将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数；

所述存储模块，用于将所述每个数组块对应的一个 32 位二进制数进行存储。

12、根据权利要求 9 所述的装置，其特征在于，所述转化单元包括：

第四转化模块，用于将第二多个二进制数的每 8 个相邻的二进制数

转化为一个单字节编码数值，生成第二字符数组；

第五转化模块，用于将所述第四转化模块得到的第二字符数组转化为待发送字符串；其中，所述第二字符数组中的一个元素对应待发送字符串中的一个字符的单字节编码数值。

13、一种通信的解密的装置，其特征在于，包括：

接收单元，用于接收发送端发送的待处理信息；

解码单元，用于将所述接收单元接收的待处理信息进行传输解码，得到第一字符串；

转化单元，用于将所述第一字符串转化为第一多个二进制数进行存储；

解密单元，用于按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数；

所述转化单元，还用于将所述第二多个二进制数转化为第二字符串。

14、根据权利要求 13 的装置，其特征在于，所述转化单元包括：

第一转化模块，用于将所述待解密的第一字符串转化为第一字符数组；其中，所述第一字符数组中的一个元素对应第三字符串中的一个字符的单字节编码数值；

分割模块，用于按照预设值，将所述第一转化模块得到的字符数组内的元素分割成若干个数组块；其中，每个数组块包括预设值数量的元素；

第二转化模块，用于将每个数组块中的元素分别转化成 8 位二进制数；

存储模块，用于将每个数组块对应的多个 8 位二进制数进行存储。

15、根据权利要求 14 所述的装置，其特征在于，所述分割模块用于按照所述第一字符数组内的元素排列情况，依次将相邻的 4 个元素划分

为一个数组块;

所述第二转化模块，用于将每个数组块内的 4 个元素分别转化为 8 位二进制数，并将每个数组块对应的 4 个 8 位二进制数合并为 1 个 32 位二进制数;

所述存储模块，用于将所述每个数组块对应的一个 32 位二进制数进行存储。

16、根据权利要求 13 所述的装置，其特征在于，所述转化单元包括:

第三转化模块，用于将第二多个二进制数的每 8 个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组。

第四转化模块，用于将所述第三转化模块得到的第二字符数组转化为第二字符串；其中，所述第二字符数组中的一个元素对应所述第二字符串中的一个字符的单字节编码数值。

17、一种通信的加密和解密的系统，其特征在于，包括如权利要求 9-12 任意一项所述的通信的加密装置和如权利要求 13-16 任意一项所述的通信的解密的装置。

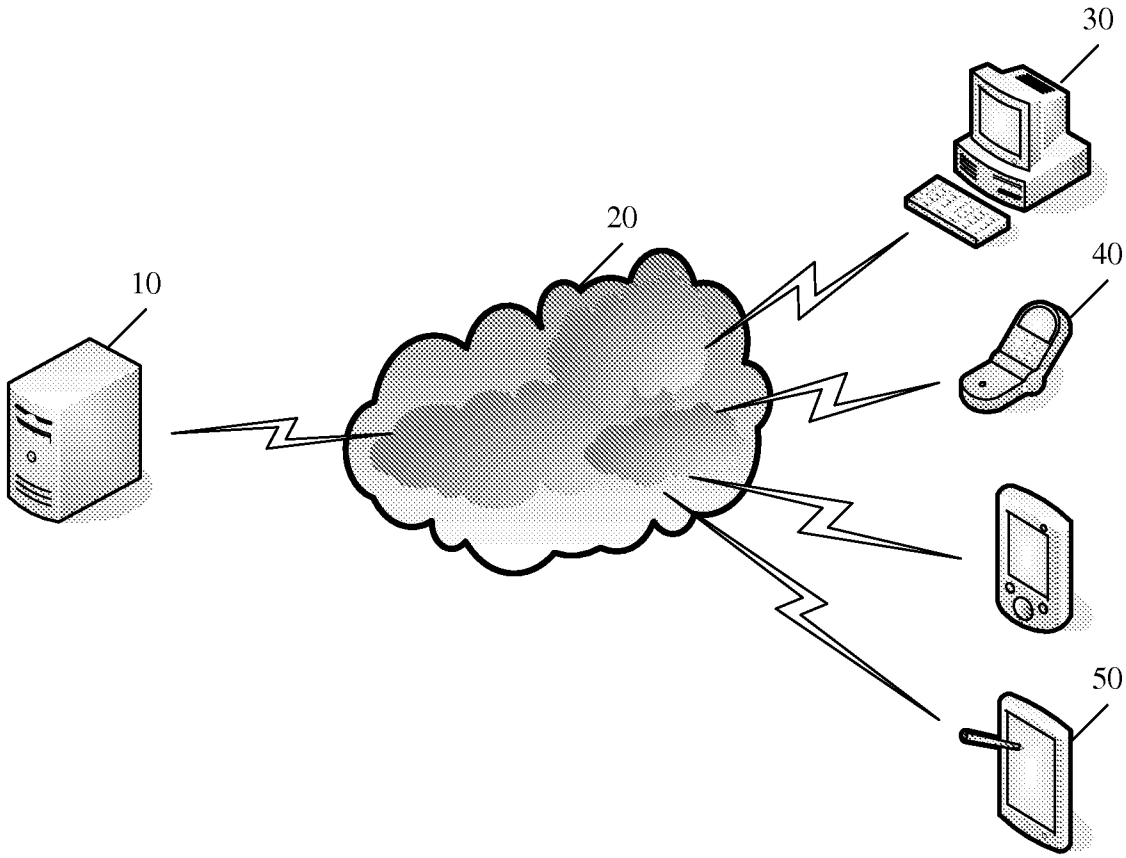


图 1

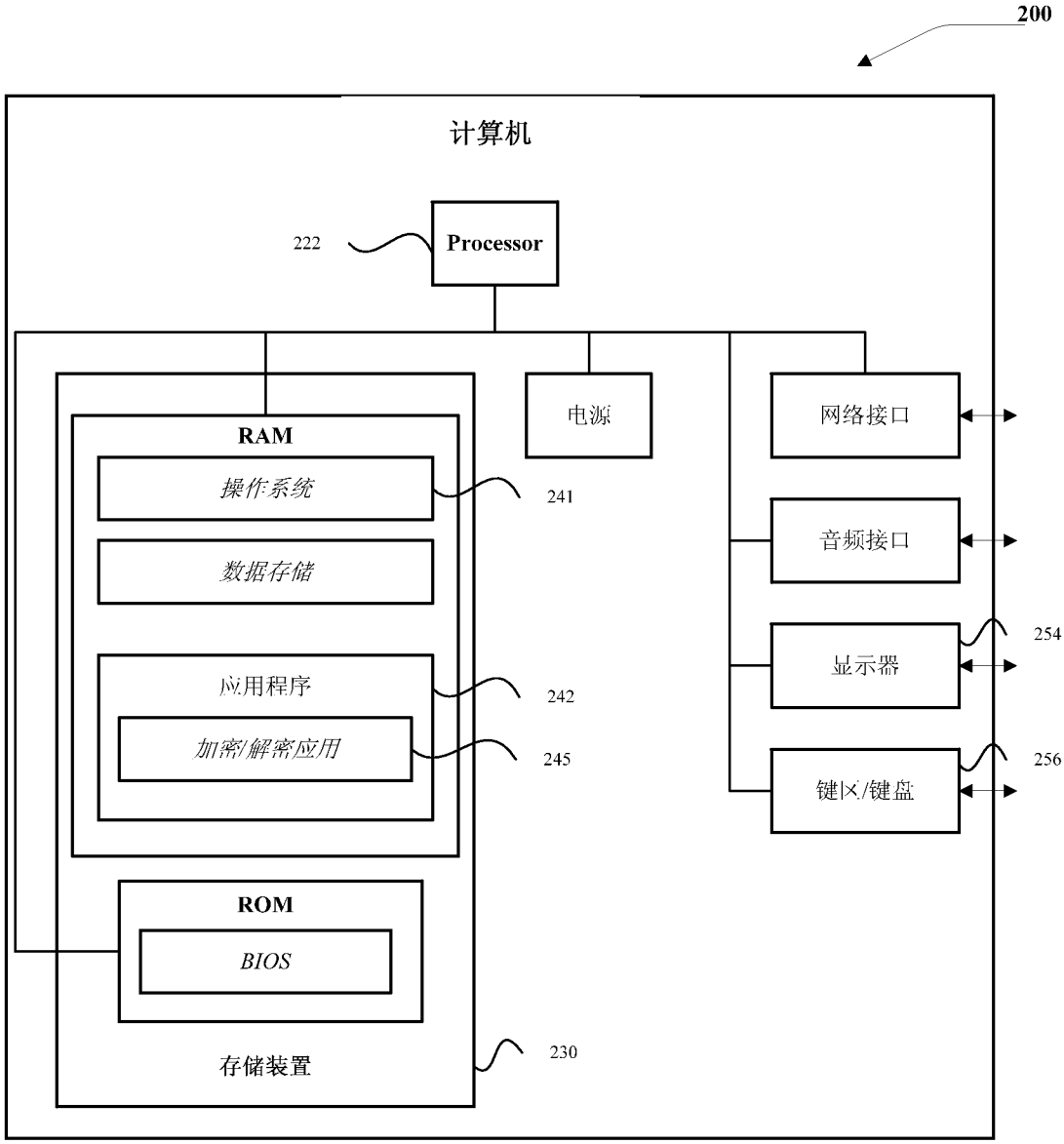

200
计算机
222
Processor
RAM
操作系统
241
数据存储
应用程序
242
加密/解密应用
245
ROM
BIOS
存储装置
230
电源
网络接口
音频接口
显示器
254
键区/键盘
256

图 2

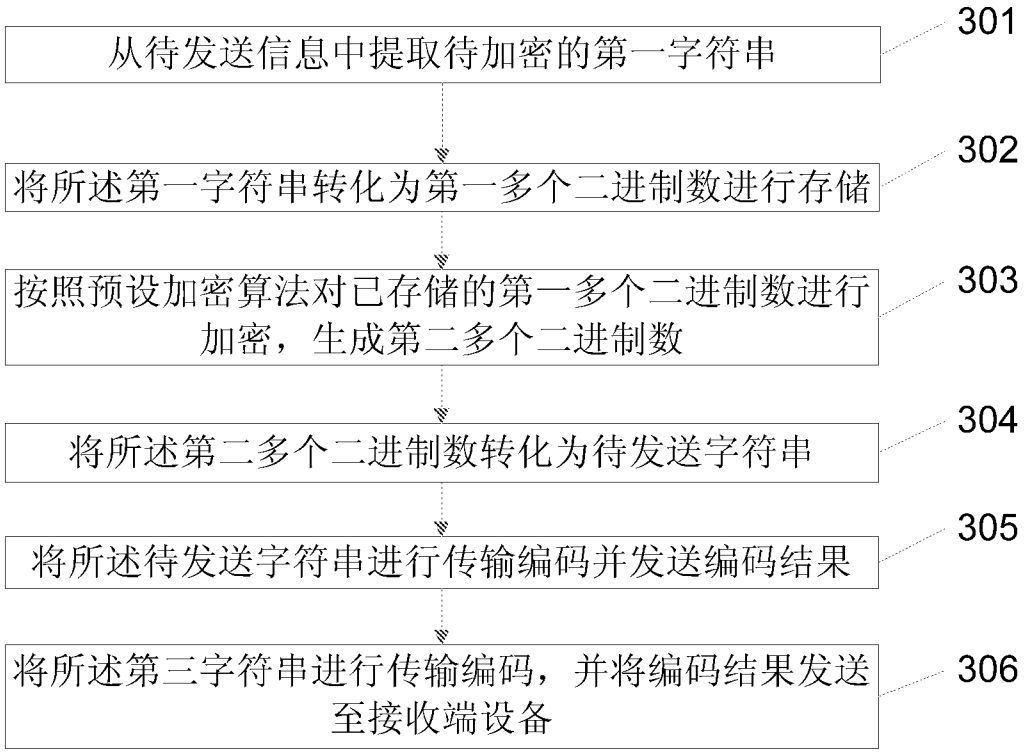

从待发送信息中提取待加密的第一字符串
301
将所述第一字符串转化为第一多个二进制数进行存储
302
按照预设加密算法对已存储的第一多个二进制数进行加密，生成第二多个二进制数
303
将所述第二多个二进制数转化为待发送字符串
304
将所述待发送字符串进行传输编码并发送编码结果
305
将所述第三字符串进行传输编码，并将编码结果发送至接收端设备
306

图 3

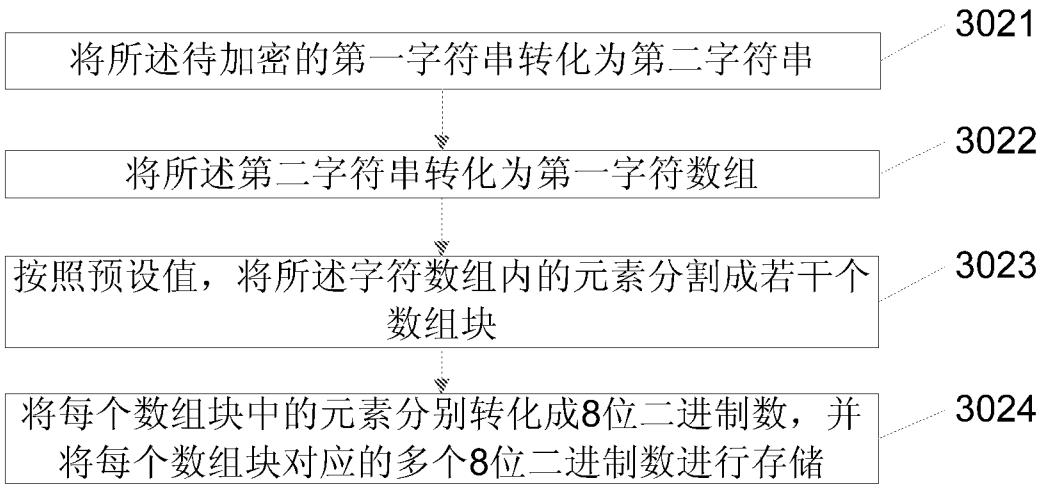

将所述待加密的第一字符串转化为第二字符串
3021
将所述第二字符串转化为第一字符数组
3022
按照预设值，将所述字符数组内的元素分割成若干个数组块
3023
将每个数组块中的元素分别转化成8位二进制数，并将每个数组块对应的多个8位二进制数进行存储
3024

图 4

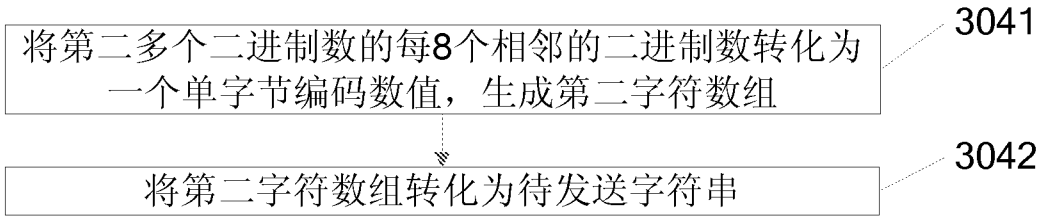

将第二多个二进制数的每8个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组
3041
将第二字符数组转化为待发送字符串
3042

图 5

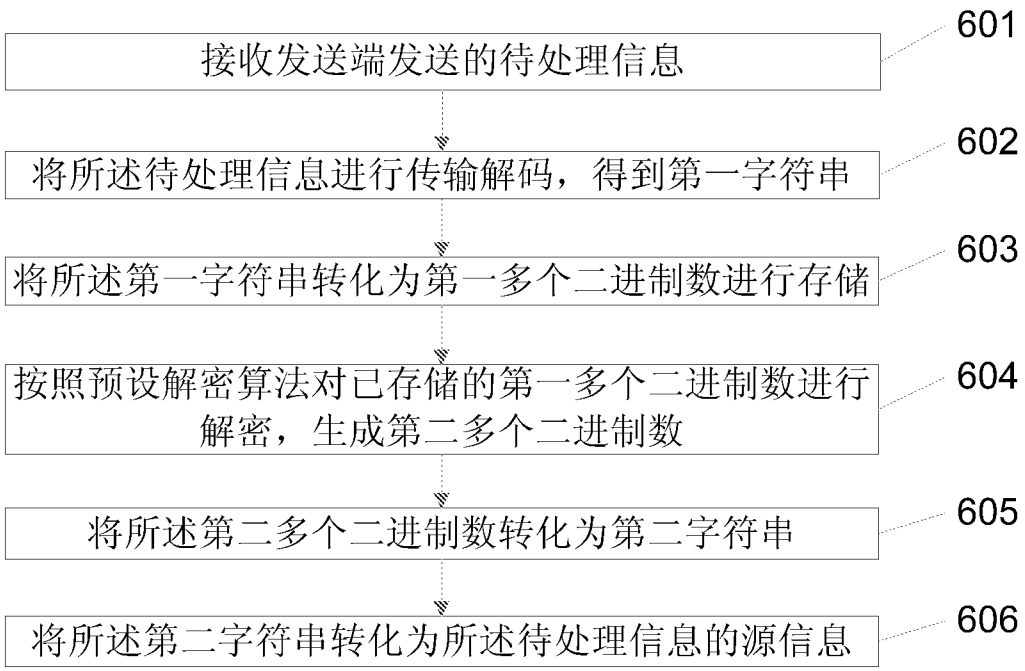

接收发送端发送的待处理信息
601
将所述待处理信息进行传输解码，得到第一字符串
602
将所述第一字符串转化为第一多个二进制数进行存储
603
按照预设解密算法对已存储的第一多个二进制数进行解密，生成第二多个二进制数
604
将所述第二多个二进制数转化为第二字符串
605
将所述第二字符串转化为所述待处理信息的源信息
606

图 6

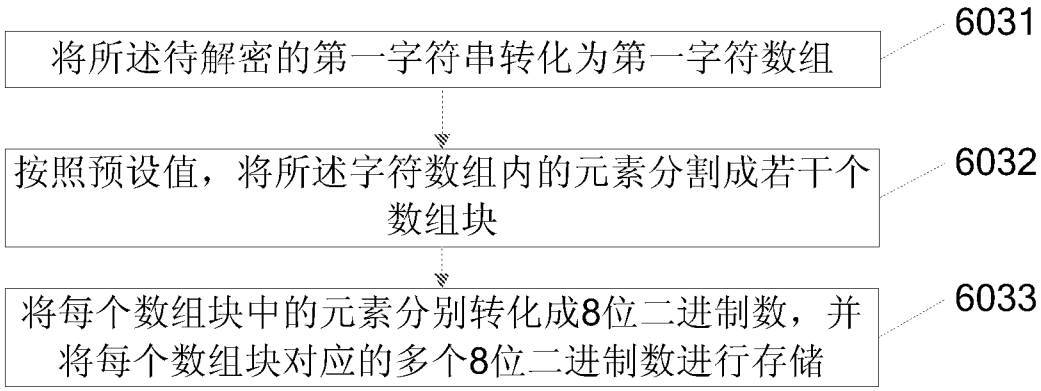

将所述待解密的第一字符串转化为第一字符数组
6031
按照预设值，将所述字符数组内的元素分割成若干个数组块
6032
将每个数组块中的元素分别转化成8位二进制数，并将每个数组块对应的多个8位二进制数进行存储
6033

图 7

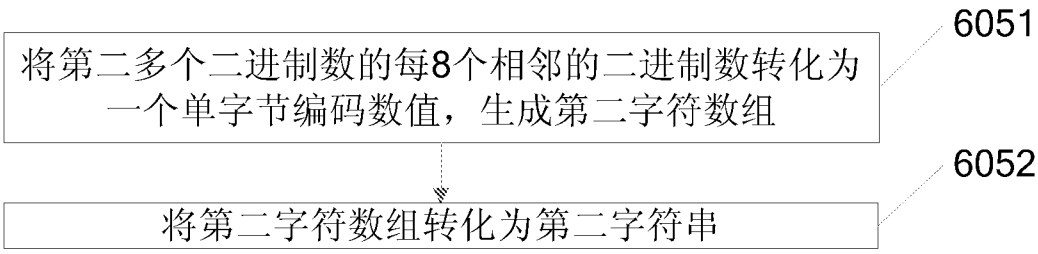

将第二多个二进制数的每8个相邻的二进制数转化为一个单字节编码数值，生成第二字符数组
6051
将第二字符数组转化为第二字符串
6052

图 8

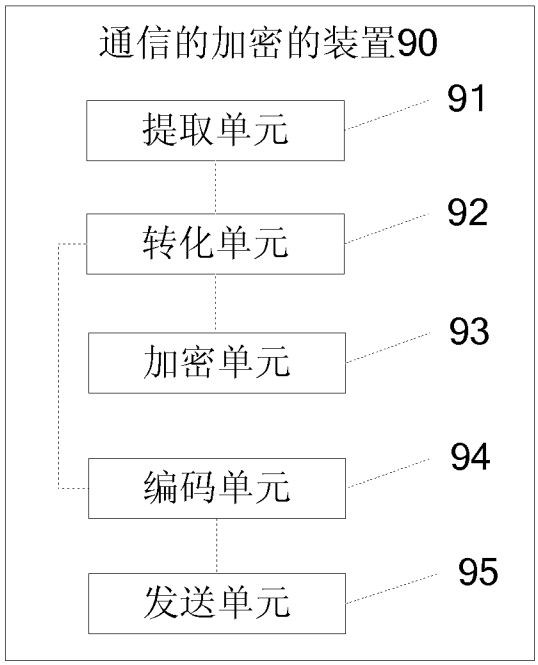

通信的加密的装置90
提取单元
91
转化单元
92
加密单元
93
编码单元
94
发送单元
95

图 9


转化单元92
第一转化模块
921
第二转化模块
922
分割模块
923
第三转化模块
924
存储模块
925

图 10


转化单元92
第一转化模块
921
第二转化模块
922
分割模块
923
第三转化模块
924
存储模块
925
第四转化模块
926
第五转化模块
927

图 11


通信的解密的装置120
接收单元
1201
解码单元
1202
转化单元
1203
解密单元
1204

图 12


转化单元1203
第一转化模块
1231
分割模块
1232
第二转化模块
1233
存储模块
1234

图 13


转化单元1203
第一转化模块
1231
分割模块
1232
第二转化模块
1233
存储模块
1234
第三转化模块
1235
第四转化模块
1236

图 14

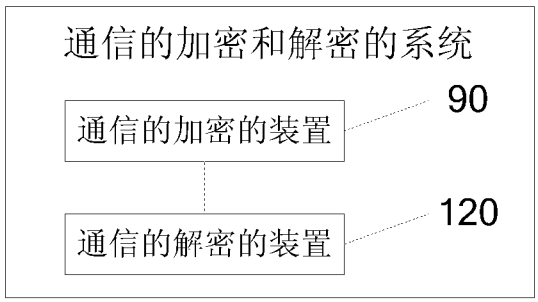


图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/083291

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/28 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04Q; H04L; H04W; G06F; H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI; EPODOC; CNKI; CNPAT: decrypt, character string, binary system, character, grouping, binary, encrypt, convert, conversion, transform, crytogram, string, stream

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1878059 A (BEIJING FORTUNE INVESTMENT CO., LTD.), 13 December 2006 (13.12.2006), description, page 1, paragraph 2 to page 2, paragraph 5 and page 4, paragraphs 4-6	1, 4-5, 9, 12-13, 16-17
A	CN 101360101 A (NINGBO SANXING ELECTRIC CO., LTD.), 04 February 2009 (04.02.2009), the whole document	1-17
A	CN 1560823 A (LI, Chunlin), 05 January 2005 (05.01.2005), the whole document	1-17
A	JP 2010-164897 A (NIPPON TELEGRAPH&TELEPHONE CORP.), 29 July 2010 (29.07.2010), the whole document	1-17

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2013 (18.11.2013)	**19 December 2013 (19.12.2013)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **WANG, Xia** Telephone No.: (86-10) **62413406**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/083291

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1878059 A	13.12.2006	None	
CN 101360101 A	04.02.2009	None	
CN 1560823 A	05.01.2005	None	
JP 2010-164897 A	29.07.2010	None	

国际检索报告

国际申请号
PCT/CN2013/083291

A. 主题的分类

H04L 9/28 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04Q; H04L; H04W; G06F; H04M

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI;EPODOC;CNKI; CNPAT: 加密，转换，解密，字符串，二进制，字，串，转化，分组，binary, encrypt, convert, conversion, transform, cryptogram, string, stream

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 1878059 A （北京财富投资有限公司）13.12 月 2006（13.12.2006）说明书第 1 页第 2 段-第 2 页第 5 段，第 4 页第 4-6 段	1, 4-5, 9, 12-13, 16-17
A	CN 101360101 A（宁波三星电气股份有限公司）04.2 月 2009（04.02.2009）全文	1-17
A	CN 1560823 A （李春林）05.1 月 2005（05.01.2005）全文	1-17
A	JP 2010-164897 A (NIPPON TELEGRAPH & TELEPHONE CORP.) 29.7 月 2010（29.07.2010）全文	1-17

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
18.11 月 2013（18.11.2013）	**19.12 月 2013 (19.12.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 王侠 电话号码：(86-10) **62413406**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/083291

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 1878059 A	13.12.2006	无	
CN 101360101 A	04.02.2009	无	
CN 1560823 A	05.01.2005	无	
JP 2010-164897 A	29.07.2010	无	