(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 106506552 B
(45)授权公告日 2020.04.03

(21)申请号 201611236415.4
(22)申请日 2016.12.28
(65)同一申请的已公布的文献号
申请公布号 CN 106506552 A
(43)申请公布日 2017.03.15
(73)专利权人 北京奇艺世纪科技有限公司
地址 100080 北京市海淀区北一街2号鸿城拓展大厦10、11层
(72)发明人 庹虎 何广 肖剑
(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 马敬 项京
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

审查员 陈莹

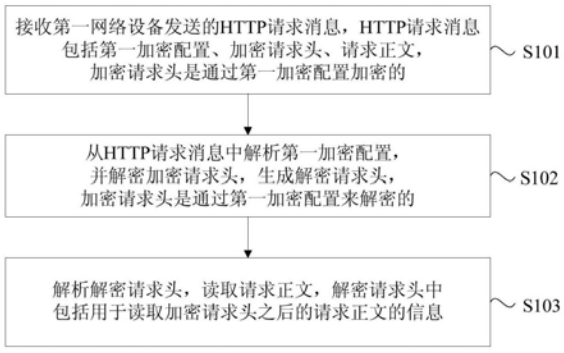
权利要求书4页 说明书12页 附图3页

(54)发明名称

一种HTTP请求传输方法及装置

(57)摘要

本发明实施例公开了一种HTTP请求传输方法及装置,所述方法包括:接收第一网络设备发送的HTTP请求消息,所述HTTP请求消息包括第一加密配置、加密请求头、请求正文,所述加密请求头是通过所述第一加密配置加密的;从所述HTTP请求消息中解析所述第一加密配置,并解密所述加密请求头,生成解密请求头,所述加密请求头是通过所述第一加密配置来解密的;解析所述解密请求头,读取所述请求正文,所述解密请求头中包括用于读取所述加密请求头之后的所述请求正文的信息。应用本发明实施例,有效解决HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持,降低资源开销。



CN 106506552 B

1.一种HTTP请求传输方法,其特征在于,所述方法包括:

第二网络设备接收第一网络设备发送的HTTP请求消息,所述HTTP请求消息包括第一加密配置、加密请求头、请求正文,所述第一加密配置包括:第一标记字符串、所述HTTP请求的版本的标识、第一加密方法的索引、第一加密密钥的索引、随机数生成器和随机填充,该第一标记字符串用于标记所述HTTP请求已加密,该随机数生成器用于生成随机密码,该随机填充用于填充解密请求头的密码,所述加密请求头是通过所述第一加密配置中的第一加密方法和第一加密密钥加密的;

从所述HTTP请求消息中解析所述第一加密配置,并解密所述加密请求头,生成解密请求头,所述加密请求头是通过所述第一加密配置中的所述第一加密方法和所述第一加密密钥所对应的第一解密方法和第一解密密钥来解密的,所述第一加密方法和所述第一加密密钥,与所述第一解密方法和所述第一解密密钥是所述第一网络设备和所述第二网络设备预先约定好的;

解析所述解密请求头,读取所述请求正文,所述解密请求头中包括用于读取所述加密请求头之后的所述请求正文的信息;

构造用于解析响应正文的响应头,通过第二加密配置中的第二加密方法和第二加密密钥 对所述响应头进行加密,生成加密响应头,所述响应正文用于响应所述请求正文;

向所述第一网络设备发送HTTP响应消息,所述HTTP响应消息包括所述第二加密配置、所述加密响应头、所述响应正文,所述第二加密配置包括:第二标记字符串、所述HTTP响应的版本的标识、所述第二加密方法的索引、所述第二加密密钥的索引、随机数生成器和随机填充,该第二标记字符串用于标记所述HTTP响应已加密,该随机数生成器用于生成随机密码,该随机填充用于填充解密响应头的密码,以使所述第一网络设备通过所述第二加密配置中的第二解密方法和第二解密密钥 解密所述加密响应头,生成解密响应头,并根据所述解密响应头读取所述响应正文,所述第二加密方法和所述第二加密密钥 ,与所述第二解密方法和所述第二解密密钥 是所述第一网络设备和所述第二网络设备预先预定好的。

2.根据权利要求1所述的方法,其特征在于,所述从所述HTTP请求消息中解析所述第一加密配置,并解密所述加密请求头,包括:

判断所述第一加密配置的第一标记字符串是否有加密标记;

若所述第一标记字符串具有所述加密标记,则根据所述第一加密配置中的加密方法索引和密钥索引,在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥;

通过所述第一解密方法和所述第一解密密钥,解密所述加密请求头。

3.一种HTTP请求传输方法,其特征在于,所述方法包括:

第一网络设备构造用于解析请求正文的请求头,通过第一加密配置中的第一加密方法和第一加密密钥对所述请求头进行加密,生成加密请求头;

向第二网络设备发送HTTP请求消息,所述HTTP请求消息包括所述第一加密配置、所述加密请求头、请求正文,所述第一加密配置包括:第一标记字符串、所述HTTP请求的版本的标识、第一加密方法的索引、第一加密密钥的索引、随机数生成器和随机填充,该第一标记字符串用于标记所述HTTP请求已加密,该随机数生成器用于生成随机密码,该随机填充用于填充解密请求头的密码,以使所述第二网络设备通过所述第一加密配置中的第一解密方

法和第一解密密钥解密所述加密请求头，生成解密请求头，并根据所述解密请求头读取所述请求正文，所述第一加密方法和所述第一加密密钥，与所述第一解密方法和所述第一解密密钥是所述第一网络设备和所述第二网络设备预先约定好的；

接收第二网络设备发送的HTTP响应消息，所述HTTP响应消息包括第二加密配置、加密响应头、响应正文，所述第二加密配置包括：第二标记字符串、所述HTTP响应的版本的标识、所述第二加密方法的索引、所述第二加密密钥的索引、随机数生成器和随机填充，该第二标记字符串用于标记所述HTTP响应已加密，该随机数生成器用于生成随机密码，该随机填充用于填充解密响应头的密码，所述加密响应头是通过所述第二加密配置中的第二加密方法和第二加密密钥 加密的；

从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，生成解密响应头，所述加密响应头是通过所述第二加密配置中的第二解密方法和第二解密密钥 来解密的，所述第二加密方法和所述第二加密密钥 ，与所述第二解密方法和所述第二解密密钥是所述第一网络设备和所述第二网络设备预先预定好的；

解析所述解密响应头，读取所述响应正文，所述解密响应头中包括用于读取所述加密响应头之后的所述响应正文的信息，所述响应正文用于响应所述请求正文。

4.根据权利要求3所述的方法，其特征在于，所述从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，包括：

判断所述第二加密配置的第二标记字符串是否有加密标记；

若所述第二标记字符串具有所述加密标记，则根据所述第二加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥，所述加密响应头是通过所述加密配置中的所述第二加密方法和所述第二加密密钥加密的；

通过所述第二解密方法和所述第二解密密钥，解密所述加密响应头。

5.一种HTTP请求传输装置，其特征在于，所述装置包括：

第一接收单元，用于第二网络设备接收第一网络设备发送的HTTP请求消息，所述HTTP请求消息包括第一加密配置、加密请求头、请求正文，所述第一加密配置包括：第一标记字符串、所述HTTP请求的版本的标识、第一加密方法的索引、第一加密密钥的索引、随机数生成器和随机填充，该第一标记字符串用于标记所述HTTP请求已加密，该随机数生成器用于生成随机密码，该随机填充用于填充解密请求头的密码，所述加密请求头是通过所述第一加密配置中的第一加密方法和第一加密密钥加密的；

第一处理单元，用于从所述HTTP请求消息中解析所述第一加密配置，并解密所述加密请求头，生成解密请求头，所述加密请求头是通过所述第一加密配置中的所述第一加密方法和所述第一加密密钥所对应的第一解密方法和第一解密密钥来解密的，所述第一加密方法和所述第一加密密钥，与所述第一解密方法和所述第一解密密钥是所述第一网络设备和所述第二网络设备预先约定好的；

第一读取单元，用于解析所述解密请求头，读取所述请求正文，所述解密请求头中包括用于读取所述加密请求头之后的所述请求正文的信息；

加密响应头单元，用于构造用于解析响应正文的响应头，通过第二加密配置中的第二加密方法和第二加密密钥 对所述响应头进行加密，生成加密响应头，所述响应正文用于响

应所述请求正文；

第一发送单元，用于向所述第一网络设备发送HTTP响应消息，所述HTTP响应消息包括所述第二加密配置、所述加密响应头、所述响应正文，所述第二加密配置包括：第二标记字符串、所述HTTP响应的版本的标识、所述第二加密方法的索引、所述第二加密密钥的索引、随机数生成器和随机填充，该第二标记字符串用于标记所述HTTP响应已加密，该随机数生成器用于生成随机密码，该随机填充用于填充解密响应头的密码，以使所述第一网络设备通过所述第二加密配置中的第二解密方法和第二解密密钥 解密所述加密响应头，生成解密响应头，并根据所述解密响应头读取所述响应正文，所述第二加密方法和所述第二加密密钥 ，与所述第二解密方法和所述第二解密密钥 是所述第一网络设备和所述第二网络设备预先预定好的。

6.根据权利要求5所述的装置，其特征在于，所述第一处理单元，还用于：

判断所述第一加密配置的第一标记字符串是否有加密标记；

若所述第一标记字符串具有所述加密标记，则根据所述第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥；

通过所述第一解密方法和所述第一解密密钥，解密所述加密请求头。

7.一种HTTP请求传输装置，其特征在于，所述装置包括：

加密请求头单元，用于第一网络设备构造用于解析请求正文的请求头，通过第一加密配置中的第一加密方法和第一加密密钥对所述请求头进行加密，生成加密请求头；

第二发送单元，用于向第二网络设备发送HTTP请求消息，所述HTTP请求消息包括所述第一加密配置、所述加密请求头、请求正文，所述第一加密配置包括：第一标记字符串、所述HTTP请求的版本的标识、第一加密方法的索引、第一加密密钥的索引、随机数生成器和随机填充，该第一标记字符串用于标记所述HTTP请求已加密，该随机数生成器用于生成随机密码，该随机填充用于填充解密请求头的密码，以使所述第二网络设备通过所述第一加密配置中的第一解密方法和第一解密密钥解密所述加密请求头，生成解密请求头，并根据所述解密请求头读取所述请求正文，所述第一加密方法和所述第一加密密钥，与所述第一解密方法和所述第一解密密钥是所述第一网络设备和所述第二网络设备预先约定好的；

第二接收单元，用于接收第二网络设备发送的HTTP响应消息，所述HTTP响应消息包括第二加密配置、加密响应头、响应正文，所述第二加密配置包括：第二标记字符串、所述HTTP响应的版本的标识、所述第二加密方法的索引、所述第二加密密钥的索引、随机数生成器和随机填充，该第二标记字符串用于标记所述HTTP响应已加密，该随机数生成器用于生成随机密码，该随机填充用于填充解密响应头的密码，所述加密响应头是通过所述第二加密配置中的第二加密方法和第二加密密钥 加密的；

第二处理单元，用于从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，生成解密响应头，所述加密响应头是通过所述第二加密配置中的第二解密方法和第二解密密钥 来解密的，所述第二加密方法和所述第二加密密钥 ，与所述第二解密方法和所述第二解密密钥 是所述第一网络设备和所述第二网络设备预先预定好的；

第二读取单元，用于解析所述解密响应头，读取所述响应正文，所述解密响应头中包括用于读取所述加密响应头之后的所述响应正文的信息，所述响应正文用于响应所述请求正

文。

8.根据权利要求7所述的装置,其特征在于,所述第二处理单元,还用于:

判断所述第二加密配置的第二标记字符串是否有加密标记;

若所述第二标记字符串具有所述加密标记,则根据所述第二加密配置中的加密方法索引和密钥索引,在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥,所述加密响应头是通过所述加密配置中的所述第二加密方法和所述第二加密密钥加密的;通过所述第二解密方法和所述第二解密密钥,解密所述加密响应头。

一种HTTP请求传输方法及装置

技术领域

[0001] 本发明涉及信息安全技术领域，尤其是涉及一种HTTP请求传输方法及装置。

背景技术

[0002] HTTP(HyperText Transfer Protocol，超文本传输协议)是一种明文的传输数据方式，HTTP请求和响应是在非加密的TCP(Transmission Control Protocol，传输控制协议)连接上进行传输的。HTTP请求是指从发送方到接收方的请求消息，在HTTP请求过程中，请求消息和响应消息都很容易被中间的代理服务器或者旁路的缓存服务器进行解析和篡改，影响请求效率和用户体验。

[0003] 现有技术通过HTTPS(Hypertext Transfer Protocol over Secure Socket Layer，以安全为目标的HTTP通道)全连接加密方案，在HTTP基础上增加了SSL(Secure Sockets Layer，安全套接层)认证和传输加密，避免了明文HTTP请求和响应过程中其他中间服务器对HTTP请求的解析和劫持。其中，HTTPS是HTTP的安全版，其主要作用可以分为两种，一种是建立一个信息安全通道，来保证数据传输的安全，另一种就是确认网站的真实性。

[0004] 但是，与明文HTTP请求相比，HTTPS请求需要单独的IP，需要额外的服务器配置以及需要购买专业证书等，这都导致资源的开销较高。

发明内容

[0005] 有鉴于此，本发明实施例的目的在于提供一种HTTP请求传输方法及装置，解决HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，降低资源开销。

[0006] 为达到上述目的，本发明实施例公开了一种HTTP请求传输方法，所述方法包括：

[0007] 接收第一网络设备发送的HTTP请求消息，所述HTTP请求消息包括第一加密配置、加密请求头、请求正文，所述加密请求头是通过所述第一加密配置加密的；

[0008] 从所述HTTP请求消息中解析所述第一加密配置，并解密所述加密请求头，生成解密请求头，所述加密请求头是通过所述第一加密配置来解密的；

[0009] 解析所述解密请求头，读取所述请求正文，所述解密请求头中包括用于读取所述加密请求头之后的所述请求正文的信息。

[0010] 可选的，所述解析所述解密请求头，读取所述请求正文之后，所述的方法还包括：

[0011] 构造用于解析响应正文的响应头，通过第二加密配置对所述响应头进行加密，生成加密响应头，所述响应正文用于响应所述请求正文；

[0012] 向所述第一网络设备发送HTTP响应消息，所述HTTP响应消息包括所述第二加密配置、所述加密响应头、所述响应正文，以使所述第一网络设备通过所述第二加密配置解密所述加密响应头，生成解密响应头，并根据所述解密响应头读取所述响应正文。

[0013] 可选的，所述从所述HTTP请求消息中解析所述第一加密配置，并解密所述加密请求头，包括：

[0014] 判断所述第一加密配置的第一标记字符串是否有加密标记；

[0015] 若所述第一标记字符串具有所述加密标记，则根据所述第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥，所述加密请求头是通过所述加密配置中的所述第一加密方法和所述第一加密密钥加密的；

[0016] 通过所述第一解密方法和所述第一解密密钥，解密所述加密请求头。

[0017] 本发明实施例还公开了另一种HTTP请求传输方法，所述方法包括：

[0018] 构造用于解析请求正文的请求头，通过第一加密配置对所述请求头进行加密，生成加密请求头；

[0019] 向第二网络设备发送HTTP请求消息，所述HTTP请求消息包括所述第一加密配置、所述加密请求头、请求正文，以使所述第二网络设备通过所述第一加密配置解密所述加密请求头，生成解密请求头，并根据所述解密请求头读取所述请求正文。

[0020] 可选的，所述向第二网络设备发送HTTP请求消息之后，所述的方法还包括：

[0021] 接收第二网络设备发送的HTTP响应消息，所述HTTP响应消息包括第二加密配置、加密响应头、响应正文，所述加密响应头是通过所述第二加密配置加密的；

[0022] 从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，生成解密响应头，所述加密响应头是通过所述第二加密配置来解密的；

[0023] 解析所述解密响应头，读取所述响应正文，所述解密响应头中包括用于读取所述加密响应头之后的所述响应正文的信息，所述响应正文用于响应所述请求正文。

[0024] 可选的，所述从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，包括：

[0025] 判断所述第二加密配置的第二标记字符串是否有加密标记；

[0026] 若所述第二标记字符串具有所述加密标记，则根据所述第二加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥，所述加密响应头是通过所述加密配置中的所述第二加密方法和所述第二加密密钥加密的；

[0027] 通过所述第二解密方法和所述第二解密密钥，解密所述加密响应头。

[0028] 本发明实施例还公开了一种HTTP请求传输装置，所述装置包括：

[0029] 第一接收单元，用于接收第一网络设备发送的HTTP请求消息，所述HTTP请求消息包括第一加密配置、加密请求头、请求正文，所述加密请求头是通过所述第一加密配置加密的；

[0030] 第一处理单元，用于从所述HTTP请求消息中解析所述第一加密配置，并解密所述加密请求头，生成解密请求头，所述加密请求头是通过所述第一加密配置来解密的；

[0031] 第一读取单元，用于解析所述解密请求头，读取所述请求正文，所述解密请求头中包括用于读取所述加密请求头之后的所述请求正文的信息。

[0032] 可选的，所述装置还包括：

[0033] 加密响应头单元，用于构造用于解析响应正文的响应头，通过第二加密配置对所述响应头进行加密，生成加密响应头，所述响应正文用于响应所述请求正文；

[0034] 第一发送单元，用于向所述第一网络设备发送HTTP响应消息，所述HTTP响应消息

包括所述第二加密配置、所述加密响应头、所述响应正文，以使所述第一网络设备通过所述第二加密配置解密所述加密响应头，生成解密响应头，并根据所述解密响应头读取所述响应正文。

[0035] 可选的，所述第一处理单元，还用于：

[0036] 判断所述第一加密配置的第一标记字符串是否有加密标记；

[0037] 若所述第一标记字符串具有所述加密标记，则根据所述第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥，所述加密请求头是通过所述加密配置中的所述第一加密方法和所述第一加密密钥加密的；

[0038] 通过所述第一解密方法和所述第一解密密钥，解密所述加密请求头。

[0039] 本发明实施例还公开了另一种HTTP请求传输装置，所述装置包括：

[0040] 加密请求头单元，用于构造用于解析请求正文的请求头，通过第一加密配置对所述请求头进行加密，生成加密请求头；

[0041] 第二发送单元，用于向第二网络设备发送HTTP请求消息，所述HTTP请求消息包括所述第一加密配置、所述加密请求头、请求正文，以使所述第二网络设备通过所述第一加密配置解密所述加密请求头，生成解密请求头，并根据所述解密请求头读取所述请求正文。

[0042] 可选的，所述装置还包括：

[0043] 第二接收单元，用于接收第二网络设备发送的HTTP响应消息，所述HTTP响应消息包括第二加密配置、加密响应头、响应正文，所述加密响应头是通过所述第二加密配置加密的；

[0044] 第二处理单元，用于从所述HTTP响应消息中解析所述第二加密配置，并解密所述加密响应头，生成解密响应头，所述加密响应头是通过所述第二加密配置来解密的；

[0045] 第二读取单元，用于解析所述解密响应头，读取所述响应正文，所述解密响应头中包括用于读取所述加密响应头之后的所述响应正文的信息，所述响应正文用于响应所述请求正文。

[0046] 可选的，所述第二处理单元，还用于：

[0047] 判断所述第二加密配置的第二标记字符串是否有加密标记；

[0048] 若所述第二标记字符串具有所述加密标记，则根据所述第二加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥，所述加密响应头是通过所述加密配置中的所述第二加密方法和所述第二加密密钥加密的；

[0049] 通过所述第二解密方法和所述第二解密密钥，解密所述加密响应头。

[0050] 由上述的技术方案可见，本发明实施例提供的一种HTTP请求传输方法及装置，通过对第一网络设备发送的HTTP请求消息中的请求头进行加密，生成加密请求头，并通过第一网络设备发送的HTTP请求消息中第一加密配置，对加密请求头进行解密，从而读取加密请求头之后的请求正文的信息，有效解决了HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，降低资源开销。当然，实施本发明的任一产品或方法必不一定需要同时达到以上所述的所有优点。

附图说明

[0051] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0052] 图1为本发明实施例提供的一种HTTP请求传输方法的一种流程图；

[0053] 图2为本发明实施例提供的一种HTTP请求传输方法的另一种流程图；

[0054] 图3为本发明实施例提供的一种HTTP请求传输方法的基本流程图；

[0055] 图4为本发明实施例提供的一种HTTP请求传输装置的第一种结构图；

[0056] 图5为本发明实施例提供的一种HTTP请求传输装置的第二种结构图；

[0057] 图6为本发明实施例提供的一种HTTP请求传输装置的第三种结构图；

[0058] 图7为本发明实施例提供的一种HTTP请求传输装置的第四种结构图。

具体实施方式

[0059] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0060] 由于普通的HTTP请求和响应是在非加密的TCP(Transmission Control Protocol，传输控制协议)连接上进行传输的，具体过程包括：首先，根据客户端输入的网址，建立TPC连接；其次，客户端向服务器端发送HTTP请求，客户端发送HTTP请求头消息、请求正文；再次，服务器会做出应答，服务器向客户端发送响应头消息；最后，服务器关闭TCP连接。但是，在这个过程中，请求消息和响应消息都很容易被中间的代理服务器或者旁路的缓存服务器进行解析和篡改，影响请求效率和用户体验。因此，本发明实施例提供了一种HTTP请求传输方法及装置，以下分别进行详细说明。

[0061] 参见图1，图1为本发明实施例提供的一种HTTP请求传输方法的一种流程图，包括如下步骤：

[0062] S101，接收第一网络设备发送的HTTP请求消息，HTTP请求消息包括第一加密配置、加密请求头、请求正文，加密请求头是通过第一加密配置加密的。

[0063] 具体的，第一网络设备发送的HTTP请求消息包括第一加密配置、加密请求头、请求正文。通过TCP连接，将HTTP请求消息发给第二网络设备，以使第二网络设备接收该HTTP请求消息，并处理该HTTP请求消息。具体的请求格式，例如可以是表1所示的请求格式：第一加密配置和加密请求头(Encrypted Header)之间、加密请求头(Encrypted Header)和请求正文(Body)之间都用换行符“\r\n”分割，加密请求头(Encrypted Header)和请求正文(Body)之间保留一行空行(Empty Line)，它表示加密请求头已经结束，接下来的是请求正文(Body)。第一加密配置包括第一标记字符串(Magic)、版本号(Ver)、加密方法索引(Alg)、密钥索引(Keyidx)、随机数生成器(Rand)、随机填充(Random Padding)。这里，对HTTP请求头进行加密，因为加密请求头不易被破解，解决中间人劫持、缓存HTTP内容的烦扰。

[0064] 表1

[0065]

Magic	Ver	Alg	Keyidx	Rand
Random Padding				
Encrypted Header				“\r\n”
Empty Line（nothing）				“\r\n”
Body				

[0066] 其中，第一标记字符串(Magic)就是把HTTP请求消息中前几个字符做标记，作用是在解密前先判断有没有这几个字符，就可以知道是否加密了；版本号(Ver)是该HTTP请求的版本的标识；加密方法索引(Alg)和密钥索引(Keyidx)主要是为了更快的找到用于解密加密请求头的第一解密方法和第一解密密钥；随机数生成器(Rand)是用于生成随机密码；随机填充(Random Padding)是用于填充解密请求头的密码。第一标记字符串、版本号、加密方法索引、密钥索引均由第一网络设备与第二网络设备按约定配置，随机填充长度由第一网络设备端随机选定。需要说明的是，在构造HTTP请求头和响应头的阶段，允许按标准HTTP请求头和响应头格式填入任意自定义请求头和响应头，如引入随机请求头和响应头内容，使加密后的请求头和响应头更加随机变化。

[0067] 另外，需要说明的是，在本发明实施例中所提到的第一网络设备和第二网络设备，分别指的是发送HTTP请求的发送方和接收HTTP请求接收方，例如，第一网络设备可以是客户端，第二网络设备可以是服务器端，对于满足所有网络设备条件的，均属于本发明实施例的保护范围，在此不一一举例。

[0068] S102，从HTTP请求消息中解析第一加密配置，并解密加密请求头，生成解密请求头，加密请求头是通过第一加密配置来解密的。

[0069] 具体的，从HTTP请求消息中解析第一加密配置，通过加密配置中的第一加密方法和第一加密密钥解密该加密请求头，生成解密请求头。这里，加密请求头是通过第一加密配置来加密的，同样的，加密请求头也是通过第一加密配置来解密的。由于加密请求头是通过加密配置中的第一加密方法和第一加密密钥加密的，因此加密请求头也是通过加密配置中的第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥解密的。其中，第一加密方法和第一加密密钥，与第一解密方法和第一解密密钥是第一网络设备和第二网络设备预先约定好的。

[0070] S103，解析解密请求头，读取请求正文，解密请求头中包括用于读取加密请求头之后的请求正文的信息。

[0071] 具体的，由于解密请求头中包括用于读取加密请求头之后的请求正文的信息，所以，第二网络设备通过解析解密请求头后，才能读取请求正文。这里，读取请求正文后，完成了对HTTP请求消息的接收，第二网络设备就会处理该HTTP请求消息，才能进一步对第一网络设备做出响应，以响应该HTTP请求消息。

[0072] 由此可见，本发明实施例提供的一种HTTP请求传输方法，通过对第一网络设备发送的HTTP请求消息中的请求头进行加密，生成加密请求头，并通过第一网络设备发送的

HTTP请求消息中第一加密配置，对加密请求头进行解密，从而读取加密请求头之后的请求正文的信息，有效解决了HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，而且只对请求头加密，解密效率高，开发成本低，从而降低了资源开销。

[0073] 在本发明的一个可选的实施例中，解析解密请求头，读取请求正文之后，的方法还包括：

[0074] 构造用于解析响应正文的响应头，通过第二加密配置对响应头进行加密，生成加密响应头，响应正文用于响应请求正文。

[0075] 具体的，构造用于解析响应正文的响应头，通过第二加密配置对响应头进行加密，加密响应头是通过第二加密配置中的第二加密方法和第二加密密钥加密的。这里，响应正文用于响应请求正文。对HTTP响应头进行加密，因为密文头不易破解，解决中间人劫持、缓存HTTP内容的烦扰，而且对响应头加密，解密效率高，开发成本低，降低了资源开销。

[0076] 向第一网络设备发送HTTP响应消息，HTTP响应消息包括第二加密配置、加密响应头、响应正文，以使第一网络设备通过第二加密配置解密加密响应头，生成解密响应头，并根据解密响应头读取响应正文。

[0077] 具体的，第二网络设备发送的HTTP响应消息包括第二加密配置、加密响应头、响应正文。通过TCP连接，将HTTP响应消息发给第一网络设备，以使第一网络设备接收该HTTP响应消息，并通过第二加密配置中的第二解密方法和第二解密密钥解密该加密响应头，生成解密响应头，并根据解密响应头读取响应正文。第二加密配置中的第二解密方法和第二解密密钥解，与第二加密配置中的第二加密方法和第二加密密钥，是第一网络设备和第二网络设备预先约定好的。这里，响应正文用于响应请求正文。具体的响应格式，例如，可以是与表1所示的请求格式相似的响应格式：第二加密配置和加密响应头(Encrypted Header)之间、加密响应头(Encrypted Header)和响应正文(Body)之间都用换行符“\r\n”分割，加密响应头(Encrypted Header)和响应正文(Body)之间保留一行空行，它表示加密响应头已经结束，接下来的是响应正文。这里，第二加密配置包括第二标记字符串(Magic)、版本号(Ver)、加密方法索引(Alg)、密钥索引(Keyidx)、随机数生成器(Rand)、随机填充(Random Padding)。

[0078] 其中，第二标记字符串(Magic)就是把HTTP响应消息中头几个字符做标记，作用是在解密前先判断有没有这几个字符，就可以知道是否加密了；版本号(Ver)是该HTTP响应的版本的标识；加密方法索引(Alg)和密钥索引(Keyidx)主要是为了更快的找到用于解密加密响应头的第二解密方法和第二解密密钥；随机数生成器(Rand)是用于生成随机密码；随机填充(Random Padding)是用于填充解密响应头的密码。

[0079] 在本发明实施例中，从HTTP请求消息中解析第一加密配置，并解密加密请求头，包括：

[0080] 判断第一加密配置的第一标记字符串是否有加密标记。

[0081] 这里，第一标记字符串是指对HTTP请求消息前几个字符所做的标记，在解密前先判断该HTTP请求消息前几个字符，就可以知道该HTTP请求消息是否加密了，其中，第一标记字符串由第一网络设备与第二网络设备按约定配置。

[0082] 若第一标记字符串具有加密标记，则根据第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的

第一解密方法和第一解密密钥,加密请求头是通过加密配置中的第一加密方法和第一加密密钥加密的。

[0083] 具体的,若第一标记字符串具有加密标记,则跳过第一加密配置中的随机填充,并根据第一加密配置中的加密方法索引和密钥索引,在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥;若第一标记字符串没有加密标记,则直接解析请求头,从而读取请求正文。

[0084] 通过第一解密方法和第一解密密钥,解密加密请求头。

[0085] 具体的,通过第一解密方法和第一解密密钥,解密加密请求头,生成解密请求头,解密请求头中包括用于读取加密请求头之后的请求正文的信息。

[0086] 参见图2,图2为本发明实施例提供的一种HTTP请求传输方法的另一种流程图,包括如下步骤:

[0087] S201,构造用于解析请求正文的请求头,通过第一加密配置对请求头进行加密,生成加密请求头。

[0088] 具体的,第一网络设备构造用于解析请求正文的请求头,通过第一加密配置对请求头进行加密,加密请求头是通过第一加密配置中的第一加密方法和第一加密密钥加密的。这里,加密请求头之后包括请求正文的信息。对HTTP请求头进行加密,因为加密请求头不易破解,解决中间人劫持、缓存HTTP内容的烦扰。

[0089] S202,向第二网络设备发送HTTP请求消息,HTTP请求消息包括第一加密配置、加密请求头、请求正文,以使第二网络设备通过第一加密配置解密加密请求头,生成解密请求头,并根据解密请求头读取请求正文。

[0090] 具体的,第一网络设备发送的HTTP请求消息包括第一加密配置、加密请求头、请求正文。通过TCP连接,将HTTP请求消息发给第二网络设备,以使第二网络设备接收该HTTP请求消息,并通过第一加密配置中的第一解密方法和第二解密密钥解密该加密请求头,生成解密请求头,并根据解密请求头读取请求正文。第一加密配置中的第一解密方法和第一解密密钥解,与第一加密配置中的第一加密方法和第一加密密钥,是第一网络设备和第二网络设备预先约定好的。

[0091] 具体的请求格式,例如,可以是如表2所示的请求格式:第一加密配置和加密请求头(Encrypted Header)之间、加密请求头(Encrypted Header)和请求正文(Body)之间都用换行符“\r\n”分割,加密请求头(Encrypted Header)和请求正文(Body)之间保留一行空行(Empty Line),它表示加密请求头已经结束,接下来的是请求正文(Body)。第一加密配置包括第一标记字符串(Magic)、版本号(Ver)、加密方法索引(Alg)、密钥索引(Keyidx)、随机数生成器(Rand)、随机填充(Random Padding)。这里,对HTTP请求头进行加密,因为加密请求头不易被破解,解决中间人劫持、缓存HTTP内容的烦扰。

[0092] 表2

[0093]

Magic	Ver	Alg	Keyidx	Rand
Random Padding				
Encrypted Header				“\r\n”
Empty Line（nothing）				“\r\n”
Body				

[0094] 其中，第一标记字符串(Magic)就是把HTTP请求消息中前几个字符做标记，作用是在解密前先判断有没有这几个字符，就可以知道该HTTP请求消息是否加密了；版本号(Ver)是该HTTP请求的版本的标识；加密方法索引(Alg)和密钥索引(Keyidx)主要是为了更快的找到用于解密加密请求头的第一解密方法和第一解密密钥；随机数生成器(Rand)是用于生成随机密码；随机填充(Random Padding)是用于填充解密请求头的密码。第一标记字符串、版本号、加密方法索引、密钥索引均由第一网络设备与第二网络设备按约定配置，随机填充长度由第一网络设备端随机选定。需要说明的是，在构造HTTP请求头和响应头的阶段，允许按标准HTTP请求头和响应头格式填入任意自定义请求头和响应头，如引入随机请求头和响应头内容，使加密后的请求头和响应头更加随机变化。

[0095] 另外，需要说明的是，在本发明实施例中所提到的第一网络设备和第二网络设备，分别指的是发送HTTP请求的发送方和接收HTTP请求接收方，例如，第一网络设备可以是客户端，第二网络设备可以是服务器端，对于满足所有网络设备条件的，均属于本发明实施例的保护范围，在此不一一举例。

[0096] 由此可见，本发明实施例提供的一种HTTP请求传输方法，通过HTTP请求消息中的第一加密配置，对第一网络设备发送的HTTP请求消息中的请求头进行加密，生成加密请求头，并向第二网络设备发送HTTP请求消息，以使第二网络设备通过第一加密配置解密加密请求头，从而读取请求正文，有效解决了HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，而且，只对请求头加密，解密效率高，开发成本低，降低了资源开销。

[0097] 在本发明的另一个可选的实施例中，向第二网络设备发送HTTP请求消息之后，所述的方法还包括：

[0098] 接收第二网络设备发送的HTTP响应消息，HTTP响应消息包括第二加密配置、加密响应头、响应正文，加密响应头是通过第二加密配置加密的。

[0099] 具体的，第二网络设备发送的HTTP响应消息包括第二加密配置、加密响应头、响应正文。通过TCP连接，将HTTP响应消息发给第一网络设备，以使第一网络设备接收该HTTP响应消息。

[0100] 具体的响应格式，例如，可以是与表2所示的请求格式相似的响应格式：第二加密配置和加密响应头(Encrypted Header)之间、加密响应头(Encrypted Header)和响应正文(Body)之间都用换行符“\r\n”分割，加密响应头(Encrypted Header)和响应正文(Body)之间保留一行空行，它表示加密响应头已经结束，接下来的是响应正文。这里，第二加密配置包括第二标记字符串(Magic)、版本号(Ver)、加密方法索引(Alg)、密钥索引(Keyidx)、随机

数生成器(Rand)、随机填充(Random Padding)。

[0101] 这里,对响应头加密,解密效率高,开发成本低,降低了资源开销。其中,第二标记字符串(Magic)就是把HTTP响应消息中前几个字符做标记,作用是在解密前先判断有没有这几个字符,就可以知道该HTTP响应消息是否加密了;版本号(Ver)是该HTTP响应的版本的标识;加密方法索引(Alg)和密钥索引(Keyidx)主要是为了更快的找到用于解密加密响应头的第二解密方法和第二解密密钥;随机数生成器(Rand)是用于生成随机密码;随机填充(Random Padding)是用于填充解密响应头的密码。第二标记字符串、版本号、加密方法索引、密钥索引均由第一网络设备与第二网络设备按约定配置,随机填充长度由第一网络设备端随机选定。

[0102] 从HTTP响应消息中解析第二加密配置,并解密加密响应头,生成解密响应头,加密响应头是通过第二加密配置来解密的。

[0103] 具体的,第一网络设备从HTTP响应消息中解析第二加密配置,通过加密配置中的第二加密方法和第二加密密钥解密该加密响应头,生成解密响应头。这里,加密响应头是通过第二加密配置来加密的,同样的,加密响应头也是通过第二加密配置来解密的。由于加密响应头是通过加密配置中的第二加密方法和第二加密密钥加密的,因此加密响应头也是通过加密配置中的第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥解密的。其中,第二加密方法和第二加密密钥,与第二解密方法和第二解密密钥是第一网络设备和第二网络设备预先约定好的。

[0104] 解析解密响应头,读取响应正文,解密响应头中包括用于读取加密响应头之后的响应正文的信息,响应正文用于响应请求正文。

[0105] 具体的,由于解密响应头中包括用于读取加密响应头之后的响应正文的信息,所以,第一网络设备通过解析解密响应头后,才能读取响应正文。这里,读取响应正文后,完成了对HTTP请求响应的接收,即完成了整个HTTP请求过程。

[0106] 在本发明实施例中,从HTTP响应消息中解析第二加密配置,并解密加密响应头,包括:

[0107] 判断第二加密配置的第二标记字符串是否有加密标记。

[0108] 这里,第二标记字符串是指对HTTP响应消息前几个字符所做的标记,在解密前先判断该HTTP响应消息前几个字符,就可以知道该HTTP响应消息是否加密了,其中,第一标记字符串由第一网络设备与第二网络设备按约定配置。

[0109] 若第二标记字符串具有加密标记,则根据第二加密配置中的加密方法索引和密钥索引,在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥,加密响应头是通过加密配置中的第二加密方法和第二加密密钥加密的。

[0110] 具体的,若第二标记字符串具有加密标记,则跳过第二加密配置中的随机填充,并根据第二加密配置中的加密方法索引和密钥索引,在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥;若第二标记字符串没有加密标记,则直接解析响应头,从而读取响应正文。这里,响应正文用于响应请求正文。

[0111] 通过第二解密方法和第二解密密钥,解密加密响应头。

[0112] 具体的，通过第二解密方法和第二解密密钥，解密加密响应头，生成解密响应头，解密响应头中包括用于读取加密响应头之后的响应正文的信息。

[0113] 参见图3，图3为本发明实施例提供的一种HTTP请求传输方法的基本流程图，包括如下步骤：

[0114] S301，构造请求头。

[0115] 具体的，第一网络设备构造用于解析请求正文的请求头。

[0116] S302，选择加密方法和密钥加密请求头。

[0117] 通过第一加密配置对请求头进行加密，加密请求头是通过第一加密配置中的第一加密方法和第一加密密钥加密的。这里，加密请求头之后包括请求正文的信息。对HTTP请求头进行加密，因为密文头不易破解，解决中间人劫持、缓存HTTP内容的烦扰。

[0118] S303，发送第一加密配置。

[0119] S304，发送加密请求头。

[0120] S305，发送请求正文。

[0121] 具体的，通过第一网络设备发送HTTP请求消息，包括第一加密配置、加密请求头、请求正文。

[0122] S306，接收HTTP请求消息。

[0123] 通过TCP连接，将HTTP请求消息发给第二网络设备，以使第二网络设备接收该HTTP请求消息。

[0124] S307，判断第一标记字符串是否有加密标识。

[0125] 这里，第一标记字符串是指对HTTP请求消息前几个字符所做的标记，在解密前先判断该HTTP请求消息前几个字符，就可以知道该HTTP请求消息是否加密了，其中，第一标记字符串由第一网络设备与第二网络设备按约定配置。

[0126] S308，解析加密配置。

[0127] 具体的，若第一标记字符串具有加密标记，则跳过第一加密配置中的随机填充，并根据第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥；

[0128] 若第一标记字符串没有加密标记，则直接跳到S310，解析加密请求头，从而读取请求正文。

[0129] S309，解密加密请求头。

[0130] 具体的，通过加密配置中的第一加密方法和第一加密密钥解密该加密请求头，生成解密请求头。这里，加密请求头是通过第一加密配置来加密的，同样的，加密请求头也是通过第一加密配置来解密的。由于加密请求头是通过加密配置中的第一加密方法和第一加密密钥加密的，因此加密请求头也是通过加密配置中的第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥解密的。其中，第一加密方法和第一加密密钥，与第一解密方法和第一解密密钥是第一网络设备和第二网络设备预先约定好的。

[0131] S310，解析加密请求头。

[0132] 具体的，由于解密请求头中包括用于读取加密请求头之后的请求正文的信息，所以，第二网络设备通过解析解密请求头后，才能读取请求正文。

[0133] S311，读取请求正文。

[0134] 这里，读取请求正文后，完成了对HTTP请求消息的接收，第二网络设备就会处理该HTTP请求消息，才能进一步对第一网络设备做出响应，以响应该HTTP请求消息。

[0135] 参见图4，图4为本发明实施例提供的一种HTTP请求传输装置的第一种结构图，包括：

[0136] 第一接收单元401，用于接收第一网络设备发送的HTTP请求消息，HTTP请求消息包括第一加密配置、加密请求头、请求正文，加密请求头是通过第一加密配置加密的；

[0137] 第一处理单元402，用于从HTTP请求消息中解析第一加密配置，并解密加密请求头，生成解密请求头，加密请求头是通过第一加密配置来解密的；

[0138] 第一读取单元403，用于解析解密请求头，读取请求正文，解密请求头中包括用于读取加密请求头之后的请求正文的信息。

[0139] 由此可见，本发明实施例提供的一种HTTP请求传输装置，通过对第一网络设备发送的HTTP请求消息中的请求头进行加密，生成加密请求头，并通过第一网络设备发送的HTTP请求消息中第一加密配置，对加密请求头进行解密，从而读取加密请求头之后的请求正文的信息，有效解决了HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，降低资源开销。

[0140] 参见图5，图5为本发明实施例提供的一种HTTP请求传输装置的第二种结构图，包括：

[0141] 加密响应头单元501，用于构造用于解析响应正文的响应头，通过第二加密配置对响应头进行加密，生成加密响应头，响应正文用于响应请求正文；

[0142] 第一发送单元502，用于向第一网络设备发送HTTP响应消息，HTTP响应消息包括第二加密配置、加密响应头、响应正文，以使第一网络设备通过第二加密配置解密加密响应头，生成解密响应头，并根据解密响应头读取响应正文。

[0143] 进一步的，第一处理单元402，还用于：

[0144] 判断第一加密配置的第一标记字符串是否有加密标记；

[0145] 若第一标记字符串具有加密标记，则根据第一加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第一加密方法和第一加密密钥所对应的第一解密方法和第一解密密钥，加密请求头是通过加密配置中的第一加密方法和第一加密密钥加密的；

[0146] 通过第一解密方法和第一解密密钥，解密加密请求头。

[0147] 参见图6，图6为本发明实施例提供的一种HTTP请求传输装置的第三种结构图，包括：

[0148] 加密请求头单元601，用于构造用于解析请求正文的请求头，通过第一加密配置对请求头进行加密，生成加密请求头；

[0149] 第二发送单元602，用于向第二网络设备发送HTTP请求消息，HTTP请求消息包括第一加密配置、加密请求头、请求正文，以使第二网络设备通过第一加密配置解密加密请求头，生成解密请求头，并根据解密请求头读取请求正文。

[0150] 由此可见，本发明实施例提供的一种HTTP请求传输装置，通过HTTP请求消息中的第一加密配置，对第一网络设备发送的HTTP请求消息中的请求头进行加密，生成加密请求头，并向第二网络设备发送HTTP请求消息，以使第二网络设备通过第一加密配置解密加密

请求头，从而读取请求正文，有效解决了HTTP请求过程中其他中间服务器对HTTP请求的解析和劫持，降低资源开销。

[0151] 参见图7，图7为本发明实施例提供的一种HTTP请求传输装置的第四种结构图，包括：

[0152] 第二接收单元701，用于接收第二网络设备发送的HTTP响应消息，HTTP响应消息包括第二加密配置、加密响应头、响应正文，加密响应头是通过第二加密配置加密的；

[0153] 第二处理单元702，用于从HTTP响应消息中解析第二加密配置，并解密加密响应头，生成解密响应头，加密响应头是通过第二加密配置来解密的；

[0154] 第二读取单元703，用于解析解密响应头，读取响应正文，解密响应头中包括用于读取加密响应头之后的响应正文的信息，响应正文用于响应请求正文。

[0155] 进一步的，第二处理单元702，还用于：

[0156] 判断第二加密配置的第二标记字符串是否有加密标记；

[0157] 若第二标记字符串具有加密标记，则根据第二加密配置中的加密方法索引和密钥索引，在预设的加密方法库和预设的密钥库中确定第二加密方法和第二加密密钥所对应的第二解密方法和第二解密密钥，加密响应头是通过加密配置中的第二加密方法和第二加密密钥加密的；

[0158] 通过第二解密方法和第二解密密钥，解密加密响应头。

[0159] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0160] 本说明书中的各个实施例均采用相关的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0161] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

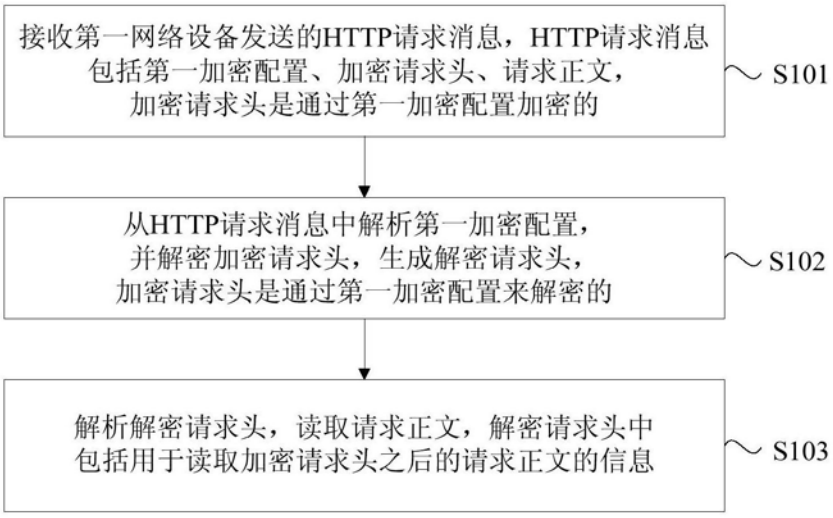

接收第一网络设备发送的HTTP请求消息，HTTP请求消息包括第一加密配置、加密请求头、请求正文，加密请求头是通过第一加密配置加密的
S101
从HTTP请求消息中解析第一加密配置，并解密加密请求头，生成解密请求头，加密请求头是通过第一加密配置来解密的
S102
解析解密请求头，读取请求正文，解密请求头中包括用于读取加密请求头之后的请求正文的信息
S103

图1

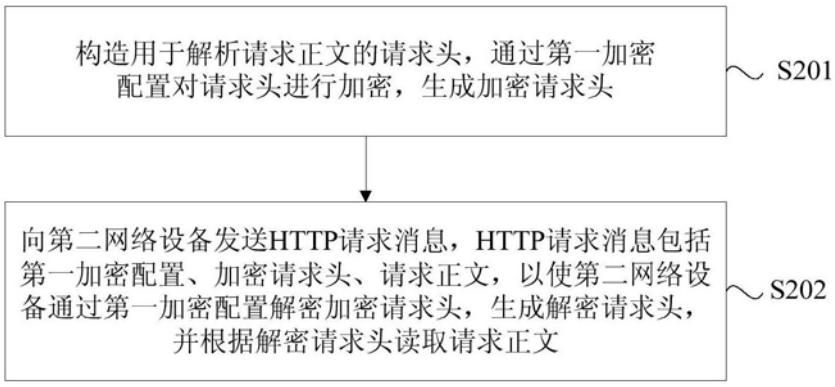

构造用于解析请求正文的请求头，通过第一加密配置对请求头进行加密，生成加密请求头
S201
向第二网络设备发送HTTP请求消息，HTTP请求消息包括第一加密配置、加密请求头、请求正文，以使第二网络设备通过第一加密配置解密加密请求头，生成解密请求头，并根据解密请求头读取请求正文
S202

图2

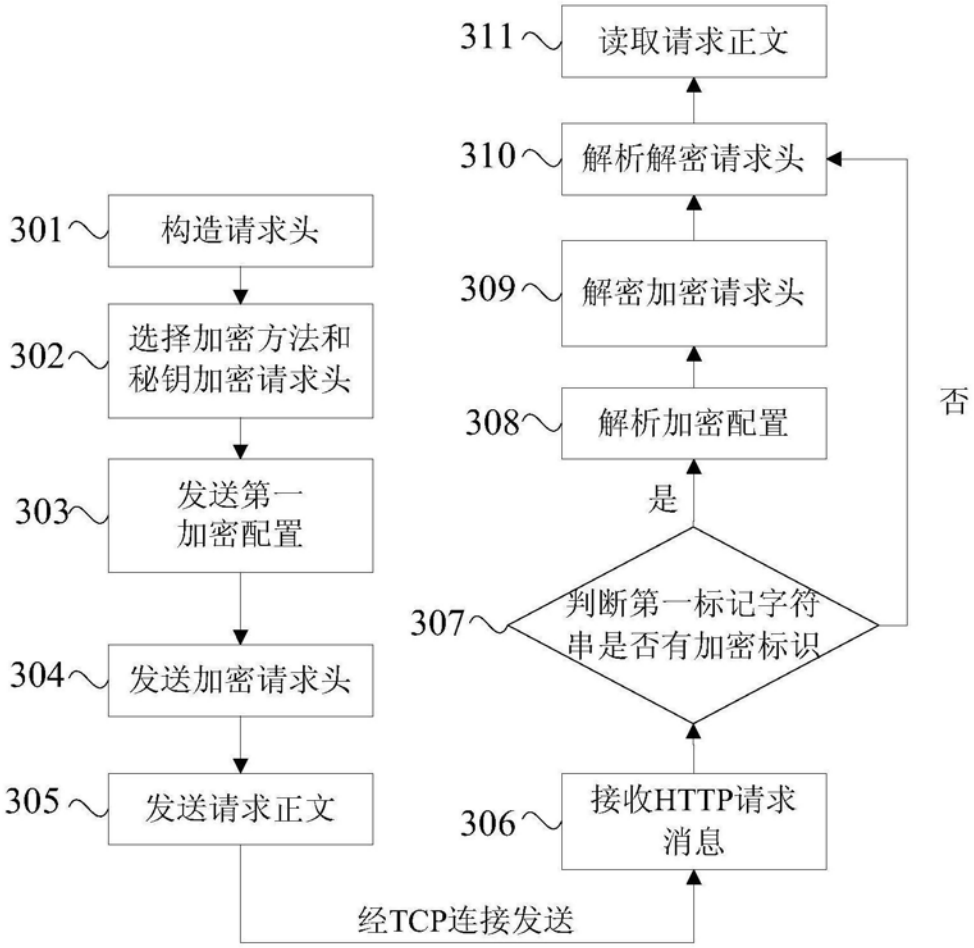

311
读取请求正文
310
解析解密请求头
309
解密加密请求头
308
解析加密配置
否
是
307
判断第一标记字符串是否有加密标识
306
接收HTTP请求消息
301
构造请求头
302
选择加密方法和秘钥加密请求头
303
发送第一加密配置
304
发送加密请求头
305
发送请求正文
经TCP连接发送

图3

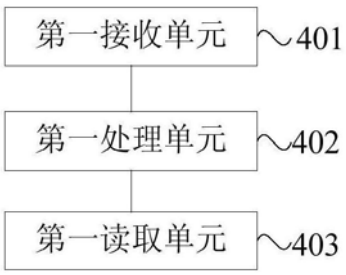

第一接收单元
401
第一处理单元
402
第一读取单元
403

图4


加密响应头单元
501
第一发送单元
502

图5

图6

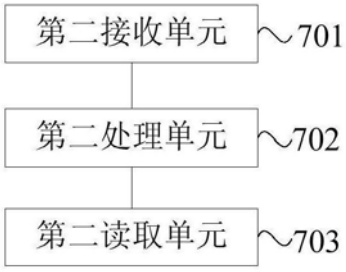


图7