**数据传输加解密方案**

**面临问题：**

数据在传输过程中数据是明文发送，存在易被拦截易破解，被攻击的等危险。

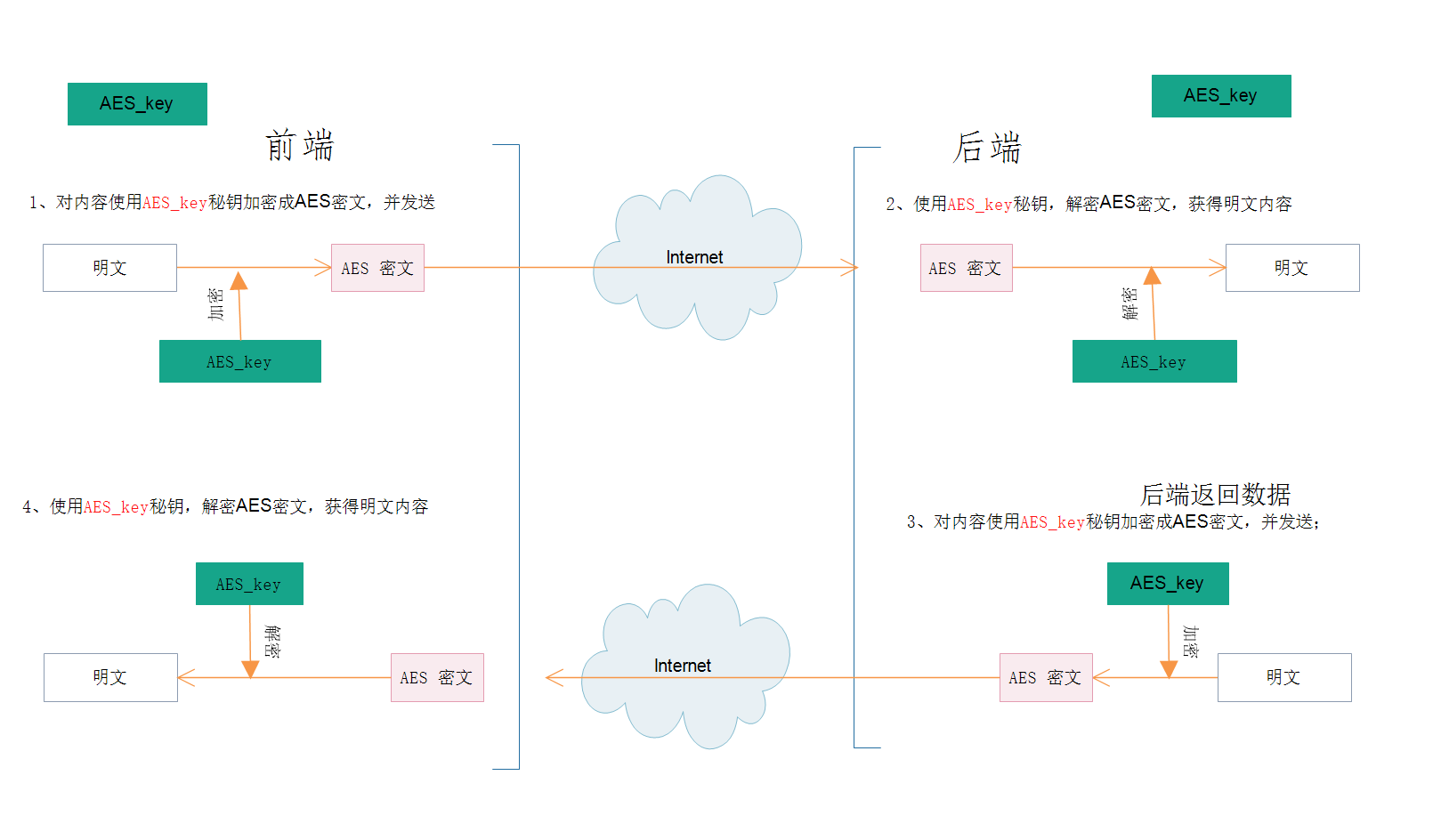
为解决这个问题，我们先来了解一下加密算法。

**对称加密**(AES算法)

AES是一种常用对称加密技术，常见的有 3 种方案，用以适应不同的场景要求，分别是AES-128、AES-192和AES-256，AES-128性能最高，AES-256安全性最高。

基于AES算法的解决思路：

前后端保存相同秘钥AES\_key，每次传输数据时，调用加密函数，生成密文发送给对方，对方接收后使用相同秘钥AES\_key解密，获得内容，如下图：



要求：加密方和解密方使用同一个密钥，对秘钥保管要求高

优点：

加密解密的运算速度快，安全性较高，资源消耗少

缺点：

密钥保存在前端，存在泄露风险；

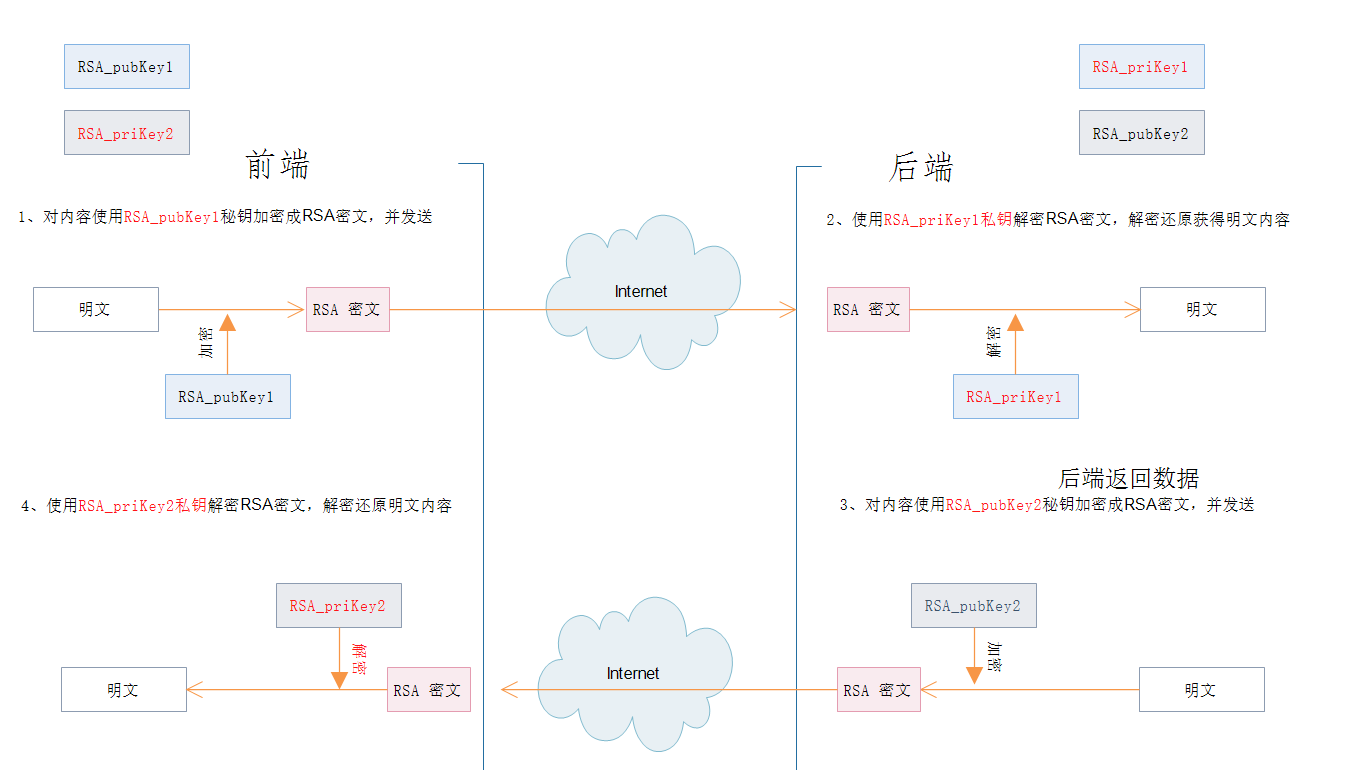
**非对称加密(RSA算法)**

RSA加密算法是一种非对称加密算法。在公开密钥加密和电子商业中RSA被广泛使用。对一极大整数做因数分解愈困难，RSA算法愈可靠，根据已经披露的文献，目前被破解的最长RSA密钥是768个二进制位，因此可以认为，1024位的RSA密钥基本安全，2048位的密钥极其安全。RSA公开密钥密码体制，使用不同的加密密钥与解密密钥。

基于RSA算法的解决思路：

前端对明文请求参数使用后端公钥RSA\_pubKey1加密成RSA密文，并发送后端，后端使用对应私钥RSA\_priKey1解密RSA密文，还原获得明文内容；

后端返回数据对内容使用前端公钥RSA\_pubKey2加密成RSA密文，并发送前端，前端使用对应私钥RSA\_priKey2解密RSA密文，还原明文内容。如下图：



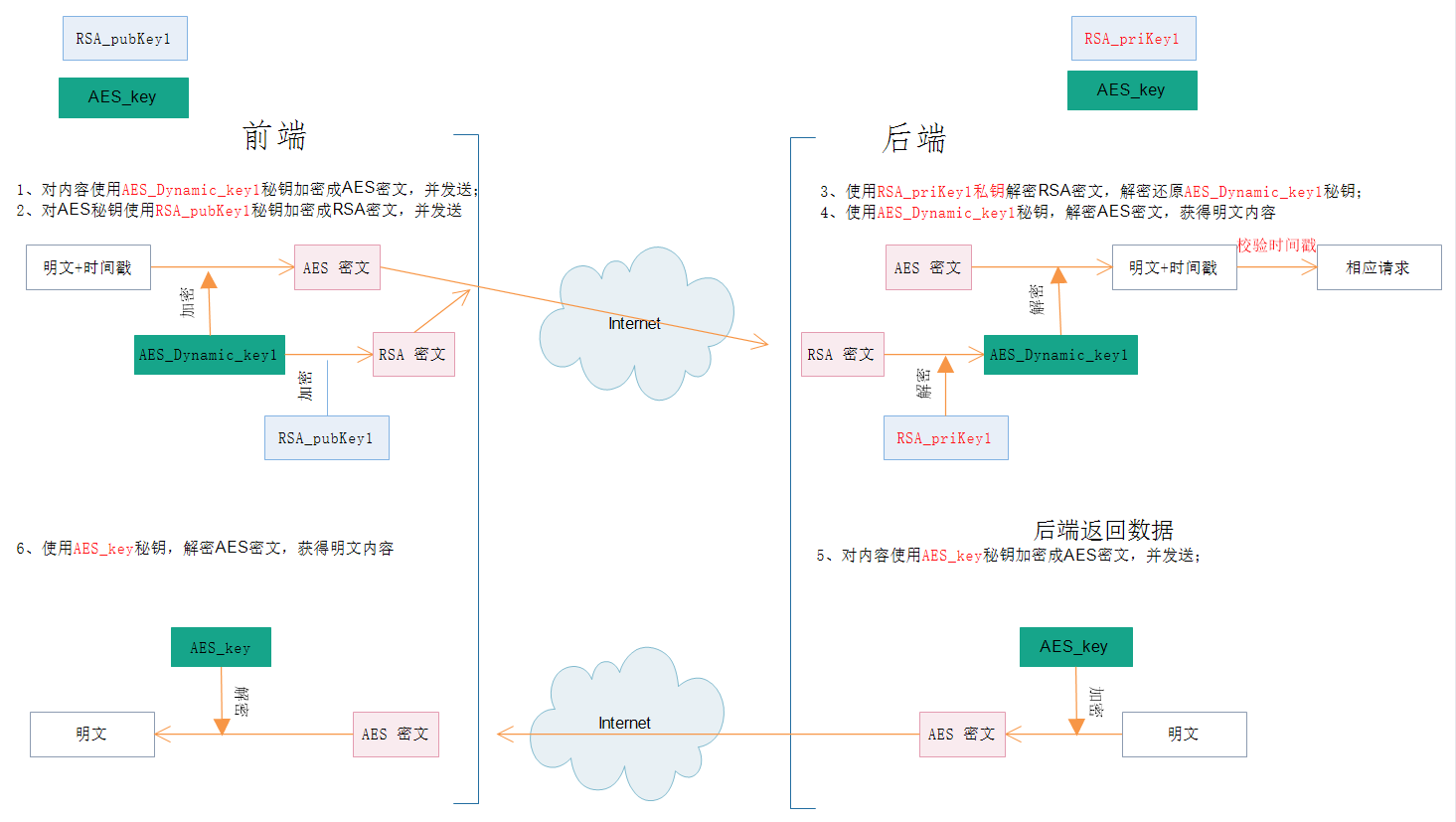
优点：只需交换公钥，不需要进行密钥传递，提高了安全性；可以进行数字签名认证

缺点：加密解密效率不高，加密内容越大消耗时间越多，一般只适用于处理小量数据（如：密钥）。

**基于 AES+RSA算法的解决方案**

结合两者的优缺点，建议以下两种方案：

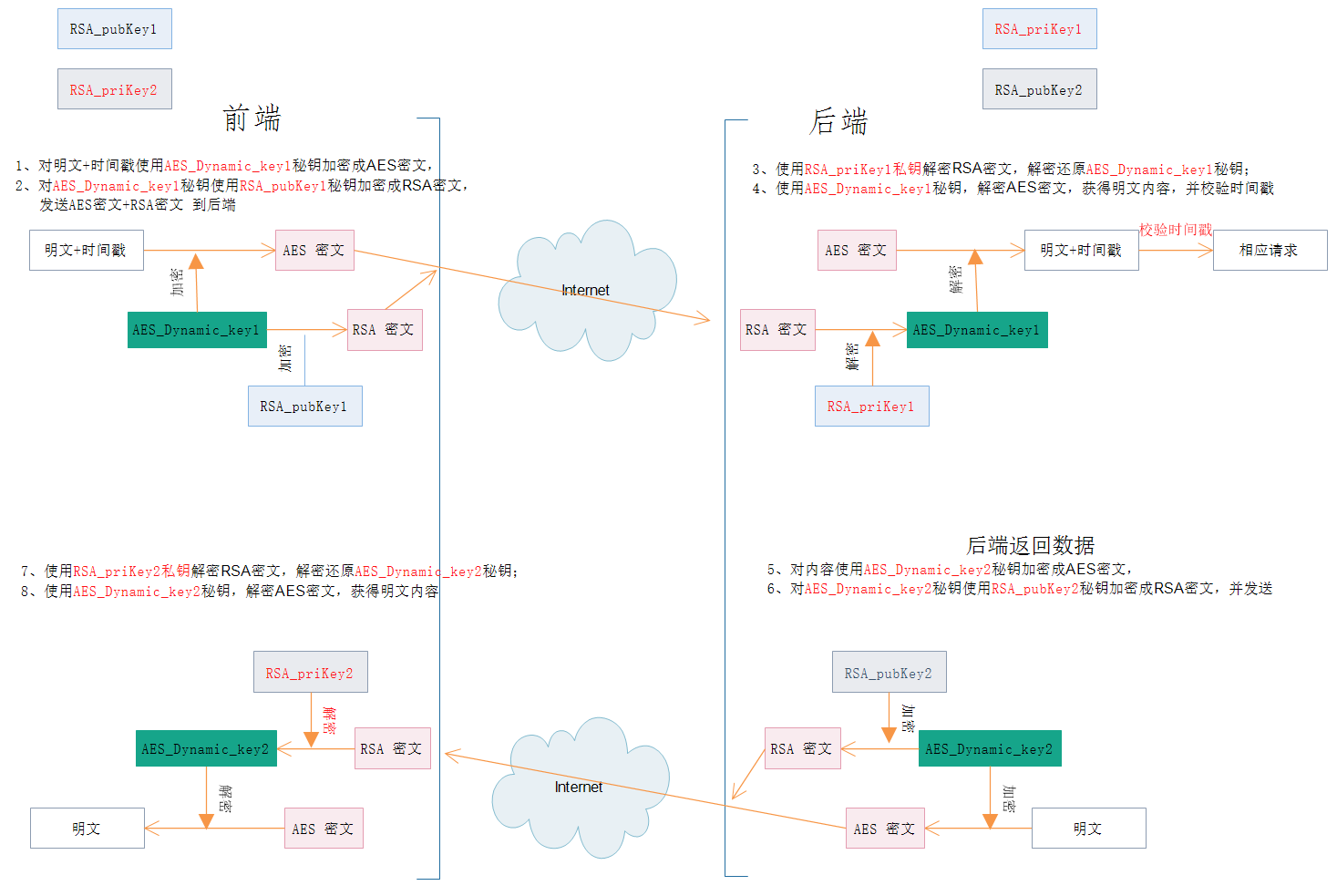
**方案1**：前端请求参数使用AES+RSA双重加密，后端服务器返回数据只使用AES算法加密。具体流程如下图：



优点：请求服务器参数数据安全性大大增加，接口的请求消耗较小

缺点：密钥AES\_key保存在前端，存在泄露风险

**方案2**、前后端请求参数和返回数据都采用AES+RSA算法加密，流程如下图：

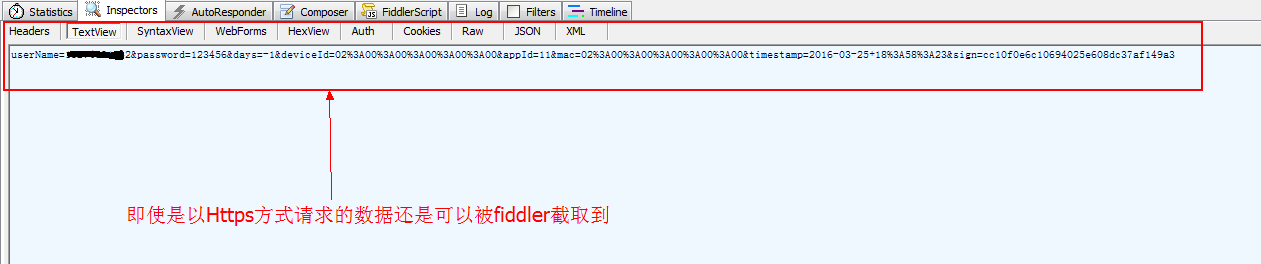


优点：安全性相对最高

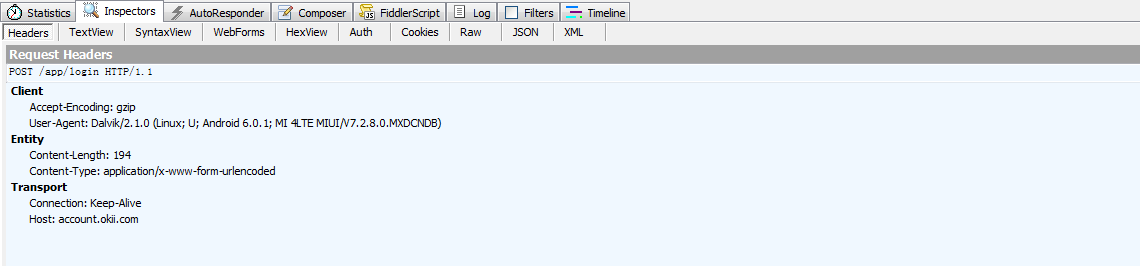
缺点：前后端交互时间消耗较大

**效果如下：**

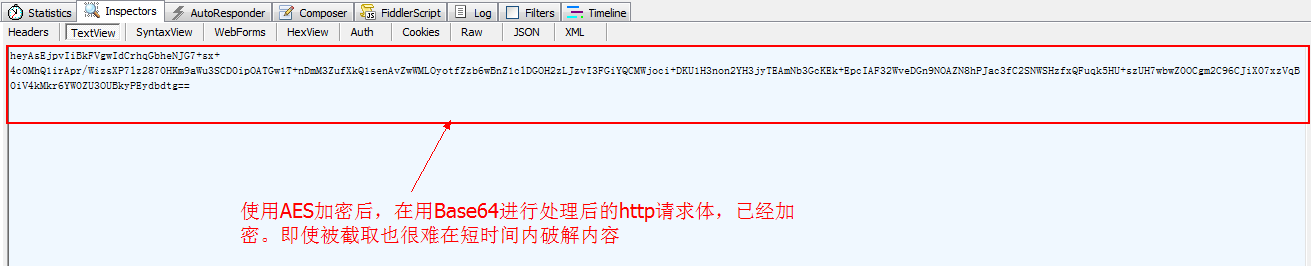
**未加密前抓包**



未加密前的请求头



**加密后抓包**



抓包获取的请求头

