Rsa 加密解密

1. 简述：

   数据传输安全是通讯领域一个很重要的方面，涉及的很多数据加密算法扮演着非常重要的角色。什么是 rsa 加密呢？传统的对称式加密，即加密解密方式客户端和服务端都知道，使用同样的密钥进行加密和解密，试想，该密钥一旦被第三方窃取了，数据就可能被截获。而 rsa 加密不一样，它是一种非对称式的数据加密方式，以下简单介绍下 rsa 加密传输流程。

2. rsa 加密解密示例

   github 为例：在加密解密信息的过程中，能让加密密钥(公钥)与解密密钥(私钥)不同，即

   (1) git 服务器要传数据给 mac 客户端(clone 操作)，mac 客户端，先根据各种算法得出与 git 服务器通讯之间所需的公钥和私钥；

   (2) mac 客户端将公钥传给 git 服务器(公钥可以让任何人知道，即使泄漏也没有关系)

   (3) git 服务器使用 mac 客户端传给公钥加密要发送的信息(某个代码仓库)，发送给 mac 客户端(clone 操作)

   (4) mac 客户端使用自己的私钥进行数据解密，得到整个项目仓库代码(clone 成功)

   这种方式，就可以很好的克服对称式被称为“非对称加密算法”

3. 强行解释

   可以观察到，从始至终，私钥都存储在信息接收方乙方，只要自己不泄露出去，私钥就没有泄露的可能

4. rsa 签名和验证

   发送数据给别人，使用私钥对传送数据进行签名，公钥交给对方进行验证签名和数据接收。

5. 总结：

   （1） 私钥用来进行加密和签名，是给自己用的

   （2） 公钥由本人公开，用于加密和验证签名，是给别人用的

   （3） 当该用户发送文件时，用私钥签名，别人用他给的公钥进行签名验证，可以保证该信息是由他本人发送的；当该用户接收文件时，别人用他的公钥进行加密，他用私钥进行解密，保证该信息只能由他本人看到