链滴

公钥与私钥、加密与签名、SSL 工作原理。

作者：snowfigure
原文链接：https://ld246.com/article/1541476260462
来源网站：链滴

公钥与私钥、加密与签名

- 使用　公钥与私钥进行安全传输的目的：
  - 我发送给你的数据必须加密，在数据的传输过程中不能被别人看到。
  - 必须保证是　我发送的数据，不是别人冒充我的。

数据	私钥	传输	公钥
010011	---> 签章	--->传输--->	验章
010011	<--- 解密	<---传输<---	加密

- 使用　公钥与私钥进行安全传输的作用：
  - 用　公钥加密的内容只能用私钥解密
  - 用　私钥签章的内容只能用公钥验章

假设 A 需要向 B 发送一份数据

- 公私钥对生成
  - A 生成公私钥对，rsa_public_a和rsa_private_a
  - B 生成公私钥对，rsa_public_b和rsa_private_b
- 公钥分发或者获取
  - A获取B的公钥rsa_public_b
  - B获取A的公钥rsa_public_a
- 数据发送
  - A准备把一份数据加密传给B
  - A使用B的公钥rsa_public_b对数据进行加密，保证数据只能B解密
  - A使用A的私钥rsa_private_a对加密的数据进行签章，保证数据是A发送的
  - A把签章后的数据通过特定传输协议发送到B端
- 数据接收
  - B收到一份来自A的报文数据
  - B使用A的公钥rsa_public_a对数据进行验章，确认数据是A发送的
  - B使用B的私钥rsa_private_b对数据进行解密
  - B获得了解密后的A发送的原始数据

```
/*    ----  参考文件  ----
      http://blog.csdn.net/it_man/article/details/24698093
 */
```

原文链接：公钥与私钥、加密与签名、SSL 工作原理。

使用公钥与私钥的目的就是实现安全的电子邮件，必须实现如下目的：
1\. 我发送给你的内容必须加密，在邮件的传输过程中不能被别人看到。
2\. 必须保证是我发送的邮件，不是别人冒充我的。
要达到这样的目标必须发送邮件的两人都有公钥和私钥。
公钥，就是给大家用的，你可以通过电子邮件发布，可以通过网站让别人下载，公钥其实是用来加/验章用的。
私钥，就是自己的，必须非常小心保存，最好加上 密码，私钥是用来解密/签章.首先就Key的所有来说，私钥只有个人拥有。
公钥与私钥的作用是：
用公钥加密的内容只能用私钥解密，用私钥加密的内容只能 用公钥解密。
比如说，我要给你发送一个加密的邮件。
首先，我必须拥有你的公钥，你也必须拥有我的公钥。
然后，我用你的公钥给这个邮件加密，这样就保证这个邮件不被别人看到，而且保证这个邮件在传过程中没有被修改。
你收到邮件后，用你的私钥就可以解密，就能看到内容。
其次我用我的私钥给这个邮件加密，发送到你手里后，你可以用我的公钥解密。因为私钥只有我手有，这样就保证了这个邮件是我发送的。
当A->B资料时，A会使用B的公钥加密，这样才能确保只有B能解开，否则普罗大众都能解开加密讯息，就是去了资料的保密性。
验证方面则是使用签 验章的机制，A传资料给大家时，会以自己的私钥做签章，如此所有收到讯息人都可以用A的公钥进行验章，便可确认讯息是由 A 发出来的了。

缩略语

缩略语	英文全名	中文解释
AES	Advanced Encryption Standard	级加密标准
CA	Certificate Authority	证书构
DES	Data Encryption Standard	据加密标准
HTTPS	Hypertext Transfer Protocol Secure	全超文本传输协议
MAC	Message Authentication Code	息验证码
MD5	Message Digest 5	消息要算法5
PKI	Public Key Infrastructure	钥基础设施
RSA	Rivest Shamir and Adleman	对称密钥算法的一种
SHA	Secure Hash Algorithm	全散列算法
SSL	Secure Sockets Layer	安全

原文链接：公钥与私钥、加密与签名、SSL 工作原理。

接层

VPN Virtual Private Network
拟专有网络

原文链接：公钥与私钥、加密与签名、SSL 工作原理。