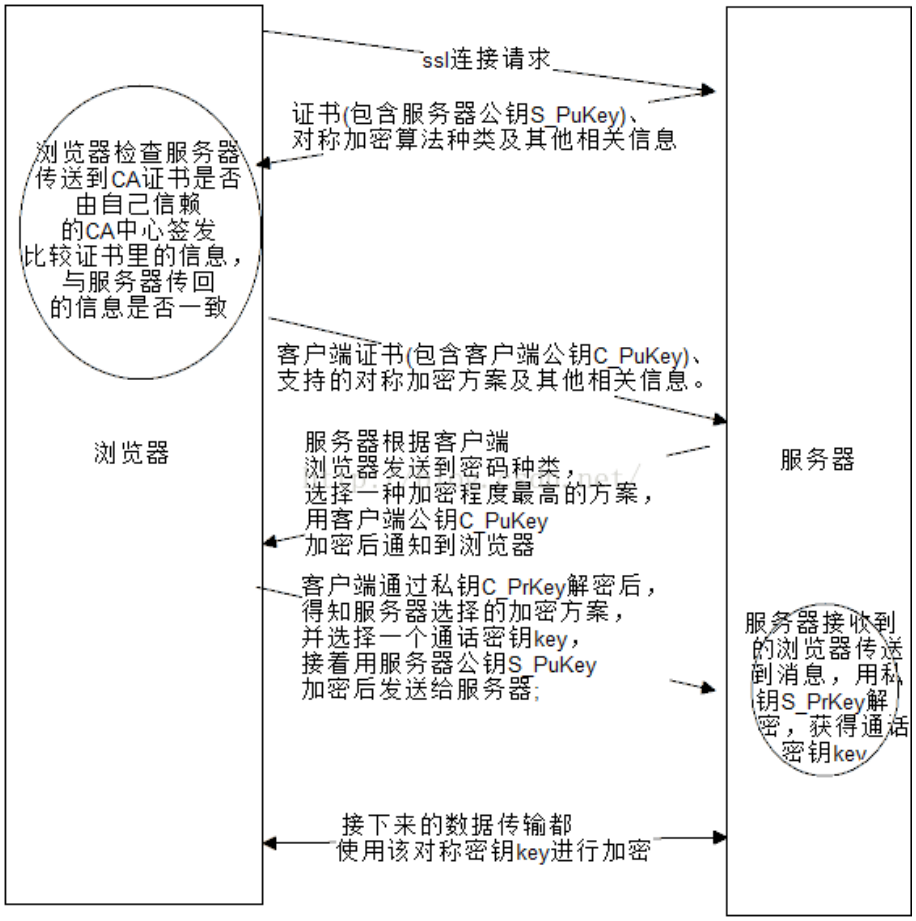
狗头

SSL

SSL协议通信过程
(1) 浏览器发送一个连接请求给服务器;服务器将自己的证书(包含服务器公钥S_PuKey)、对称加密算法种类及其他相关信息返回客户端;
(2) 客户端浏览器检查服务器传送到CA证书是否由自己信赖的CA中心签发。若是，执行4步;否则，给客户一个警告信息：询问是否继续访问。
(3) 客户端浏览器比较证书里的信息，如证书有效期、服务器域名和公钥S_PK，与服务器传回的信息是否一致，如果一致，则浏览器完成对服务器的身份认证。
(4) 服务器要求客户端发送客户端证书(包含客户端公钥C_PuKey)、支持的对称加密方案及其他相关信息。收到后，服务器进行相同的身份认证，若没有通过验证，则拒绝连接;
(5) 服务器根据客户端浏览器发送到密码种类，选择一种加密程度最高的方案，用客户端公钥C_PuKey加密后通知到浏览器;
(6) 客户端通过私钥C_PrKey解密后，得知服务器选择的加密方案，并选择一个通话密钥key，接着用服务器公钥S_PuKey加密后发送给服务器;
(7) 服务器接收到的浏览器传送到消息，用私钥S_PrKey解密，获得通话密钥key。
(8) 接下来的数据传输都使用该对称密钥key进行加密。
上面所述的是双向认证 SSL协议的具体通讯过程，服务器和用户双方必须都有证书。由此可见，SSL协议是通过非对称密钥机制保证双方身份认证，并完成建立连接，在实际数据通信时通过对称密钥机制保障数据安全性



加上了证书，同时使用了混合加密算法。

加密技术：对称加密非对称加密

https://blog.csdn.net/u013320868/article/details/54090295

在了解对称加密和非对称加密的区别之前我们先了解一下它们的定义：

对称加密（Symmetric Cryptography**），又称私钥加密**

对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key）,这种方法在密码学中叫做对称加密算法。对称加密有很多种算法，由于它效率很高，所以被广泛使用在很多加密协议的核心当中。对称加密通常使用的是相对较小的密钥，一般小于256 bit。因为密钥越大，加密越强，但加密与解密的过程越慢。如果你只用1 bit来做这个密钥，那黑客们可以先试着用0来解密，不行的话就再用1解；但如果你的密钥有1 MB大，黑客们可能永远也无法破解，但加密和解密的过程要花费很长的时间。密钥的大小既要照顾到安全性，也要照顾到效率，是一个trade-off。

非对称加密（Asymmetric Cryptography**），又称公钥加密**

1976年，美国学者Dime和Henman为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（public key）和私钥（private key）。**私钥只能由一方安全保管，不能外泄，而公钥则可以发给任何请求它的人。**非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。比如，你向银行请求公钥，银行将公钥发给你，你使用公钥对消息加密，那么只有私钥的持有人-银行才能对你的消息解密。与对称加密不同的是，银行不需要将私钥通过网络发送出去，因此安全性大大提高。

下面说一下这两种方式的使用

对称密钥加密我们从定义中应该就可以明白，它是信息的发送方和接收方都用同一个秘钥去加密和解密数据。这样做它的最大优势是加/解密速度快，适合于对大数据量进行密，但密钥管理困难。

非对称密钥加密，它需要使用“一对”密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。

非对称密钥加密的使用过程：

1. A要向B发送信息，A和B都要产生一对用于加密和解密的公钥和私钥。
2. A的私钥保密，A的公钥告诉B；B的私钥保密，B的公钥告诉A。
3. A要给B发送信息时，A用B的公钥加密信息，因为A知道B的公钥。
4. A将这个消息发给B（已经用B的公钥加密消息）。
5. B收到这个消息后，B用自己的私钥解密A的消息，其他所有收到这个报文的人都无法解密，因为只有B才有B的私钥。
6. 反过来，B向A发送消息也是一样。

从上面大家应该可以看出对称加密和非对称加密的区别，下面稍微进行一下总结：

（1） 对称加密加密与解密使用的是同样的密钥，所以速度快，但由于需要将密钥在网络传输，所以安全性不高。

（2） 非对称加密使用了一对密钥，公钥与私钥，所以安全性高，但加密与解密速度慢。

（3） **解决的办法是将对称加密的密钥使用非对称加密的公钥进行加密，然后发送出去，接收方使用私钥进行解密得到对称加密的密钥，然后双方可以使用对称加密来进行沟通。标红色的地方是重点，这是目前在通信方面最安全的做法。**

STL

红黑树：插入快还是查询快。

归并，分治，贪心等算法思想

纯虚函数：用在哪里

含有纯虚函数的类成为抽象类，不能生成对象。

i++和++i