网络传输中客户端和服务器端的数据加解密方案

目前的数据加密技术根据加密密钥类型，可分为对称加解密算法和非对称加解密算法；对称加密算法是比较传统的加密体制，通信双方在加解密过程中使用它们共享的单一密钥，算法简单，但加密速度快，目前仍是主流的密码体制之一；非对称加密算法由于加解密钥不同，密钥管理简单，公钥加密，私钥解密，在很多行业得到应用。

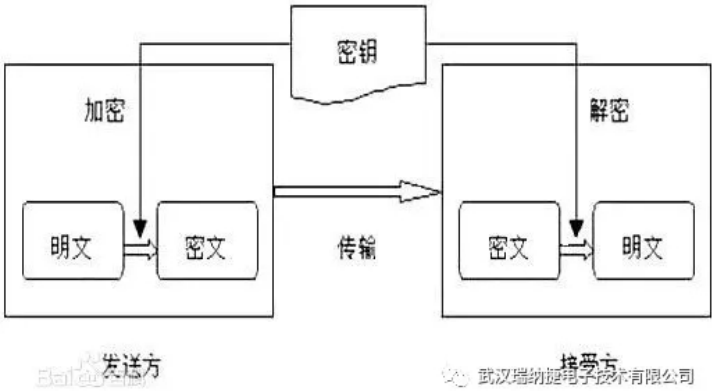
密钥是与加密算法一起用于加密某些输入(称为明文)的值。输出称为密文。密钥本质上是非常非常大的数。密钥的尺寸用位(bit)来衡量，1024 位密钥代表的数是非常巨大的。在公开密钥加密方法中，密钥的尺寸越大，密文就越安全。假定有相同的输入和相同的算法,不同的密钥会生成不同的密文。 有两种大量使用的密钥加密技术：私用密钥（对称加密）和公共密钥（非对称加密）。对称密钥加密，又称私钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。在非对称加密体系中，密钥被分解为一对。这对密钥中的任何一把都可作为公开密钥（加密密钥）通过非保密方式向他人公开，而另一把则作为私用密钥（解密密钥）加以保存。私用密钥只能由生成密钥对的贸易方掌握，公开密钥可广泛发布。

数据加解密算法

对称加密算法：DES 3DES AES SM1 SM4;

非对称加密算法：RSA1024/2048 SM2；

摘要加密算法：SM3 SHA256；



3DES 对称加密方案

1、发送方和接收方首先约定产生一个相同的管理密钥；

2、在发送方的计算机串通过随机数算法产生一个 128 位的随机密钥；

3、利用先前产生的 128 位随机密钥对明文数据进行 3DES 加密，获得相应的密文数据；

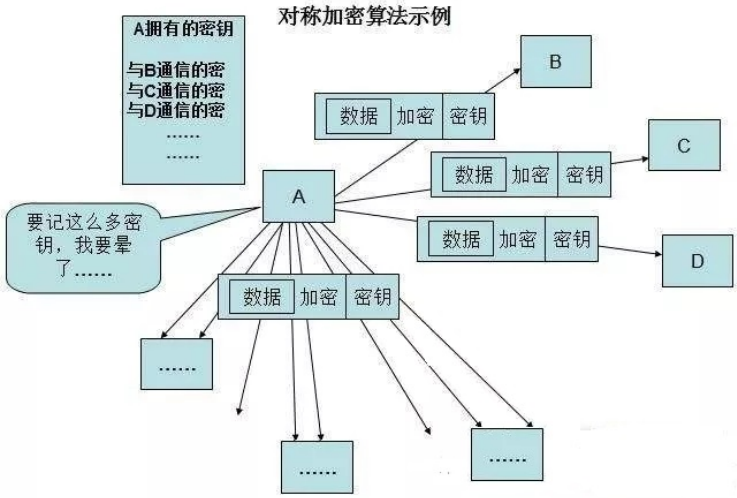
4、将 128 位随机数密钥及文件扩展名、文件类型、 有效内容长度等信息组成管理信息， 用发送方的管理密钥对管理信息加密得到包头密文 A；

5、将包头密文 A 与先前获得的数据密文拼起来组成密文数据包发送给接收方；

6、接收方收到发送方送来的密文数据包后 ，将其拆分成密文包头 A 和数据密文两项；

7、将密文包头放入密文包头缓冲区中 用接收方的管理密钥对密文包头进行解密，得到 128 位随机密钥、文件扩展各、文件类型、有效内容长度等数据；

8、利用得到的 128 位随机密钥对密文数据进行解密，得到相应的明文数据。

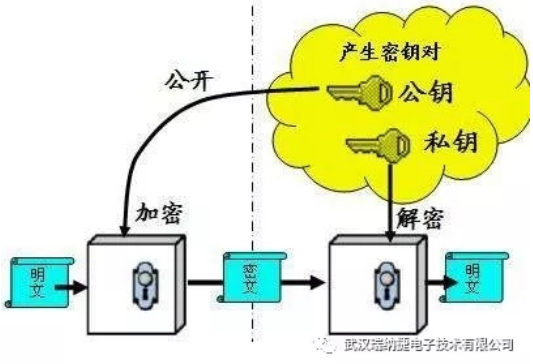


RSA 非对称密钥加密方案

1、接收方创建 RSA 密钥对，即一个公钥和一个私钥，并将公钥发送到发送方，私钥则被保存在接收方；

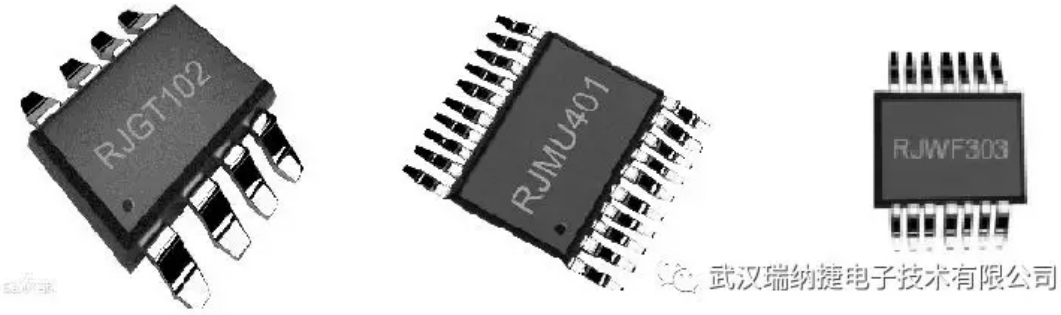
2、发送方在接收到这个公钥后，用该公钥对明文进行加密得到密文；

3、把密文通过网络传输给接收方；
4、接收方在收到密文后，用 RSA 私钥对收到的密文进行解密，最后得到明文。



推荐使用芯片

1、RJGT102 系列；
2、RJMU401 系列；



应用方向

1、网络传输中客户端和服务器端的数据加解密；
2、通讯线路上客户端和服务器的数据加解密；
3、系统内部数据传输线路上的数据加解密；