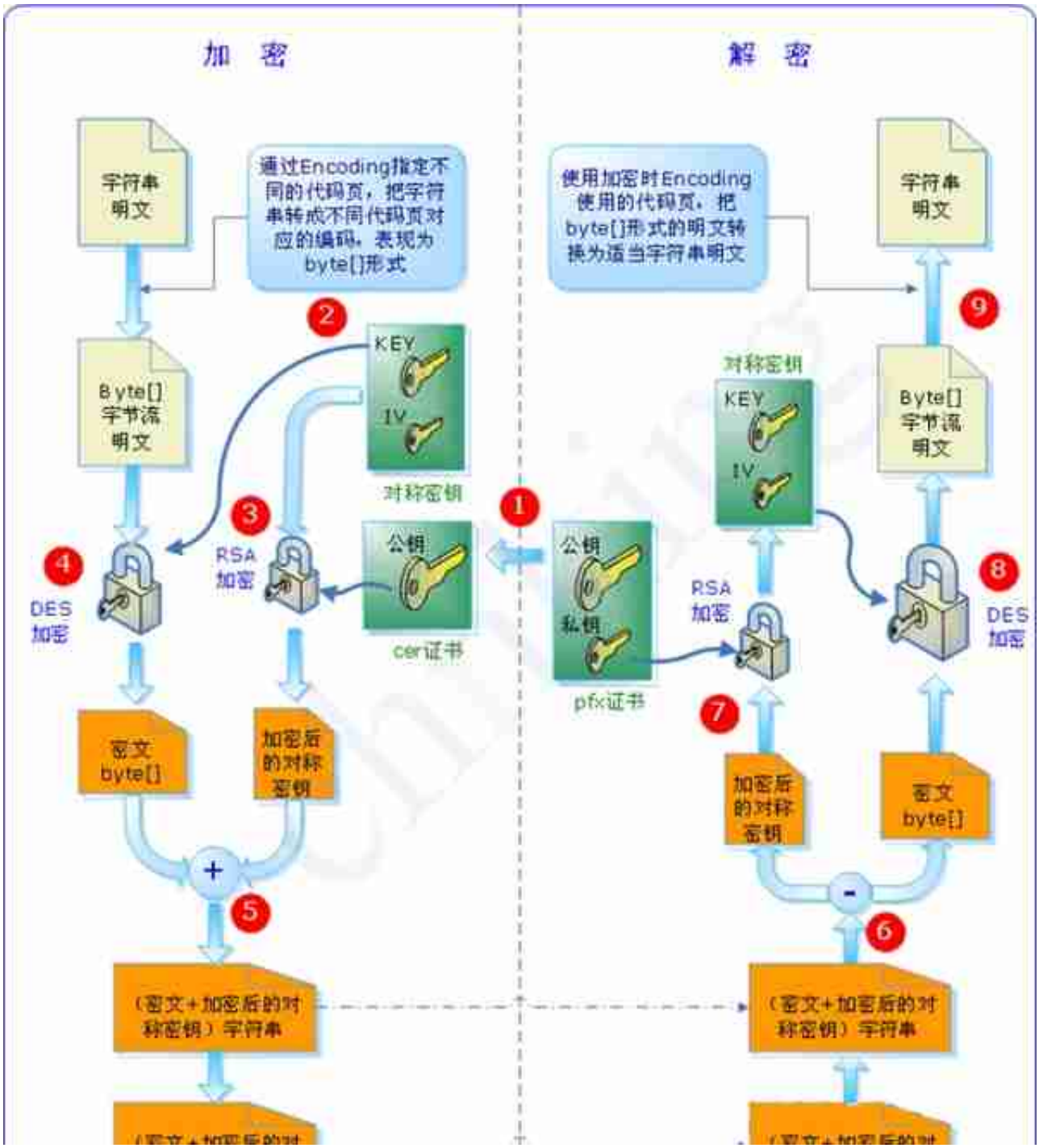
一、公钥算法与私钥算法



2、公钥算法

公钥加密算法，也就是 非对称加密算法，这种算法加密和解密的密码不一样，一个是公钥，另一个是私钥：

- 公钥和私钥成对出现
- 公开的密钥叫公钥，只有自己知道的叫私钥
- 用公钥加密（或签名）的数据只有对应的私钥可以解密

- 用私钥加密（或签名）的数据只有对应的公钥可以解密
- 如果可以用公钥解密，则必然是对应的私钥加的密
- 如果可以用私钥解密，则必然是对应的公钥加的密

公钥和私钥是相对存在。

3、钱包地址

公钥可以生成对应的唯一地址，验证发送交易的地址是否和该公钥生成的地址一致。

二、实现数据的安全传输

要实现数据的安全传输，当然就要对数据进行加密。如果使用对称加密算法，加解密使用同一个密钥，除了自己保存外，对方也要知道这个密钥，才能对数据进行解密。如果你把密钥也一起传过去，就存在密码泄漏的可能。所以我们使用非对称算法，过程如下：

①接收方 生成一对密钥，即私钥和公钥；

②然后，接收方 将公钥发送给 发送方；

③发送方用收到的公钥对数据加密，再发送给接收方；

④接收方收到数据后，使用自己的私钥解密。

以下为 RSA 结合 TripleDES 算法 加密解密过程