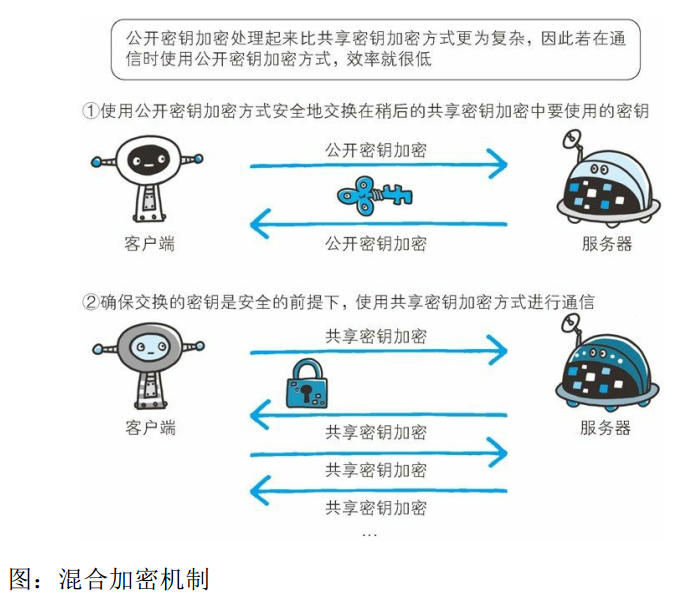
共享密钥加密：

加密和解密同用一个密钥的方式称为共享密钥加密（Common key crypto system），也被叫做对称密钥加密。

公钥加密方式：

公开密钥则可以随意发布，任何人都可以获得。发送密文的一方使用对方的公开密钥进行加密处理，对方收到后再使用自己的私有密钥进行解密。

HTTPS使用混合加密机制，



如上图，公钥加密方式（加密的是共享密钥）交换的是稍后共享密钥加密要使用的密钥。

如下图，服务器将自己的公钥发送给客户端，客户端将用于共享密钥加密的密钥使用该公钥加密后发送给服务器，这个一个交换的过程。

