**网络空间安全导论大作业（一）**

学号： 姓名：

* 对称密码学在安全中的应用

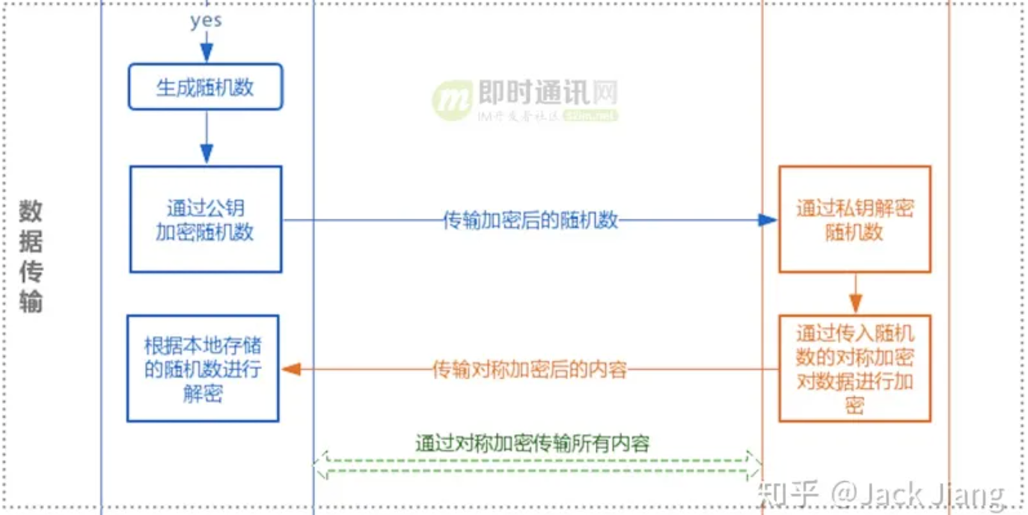
伴随着5G、物联网及大数据技术的快速发展，人们在工作、学习及生活等方面均获得很大的便捷，数据安全问题已经成为了人们关注的焦点，而保护数据的最好方法，便是对其进行加密，以防止数据内容被恶意窃取。

用于数据加密的密码体制，从密钥数量上来说，可以分为对称密码体制和非对称密码体制（公钥密码体制）。对称密码算法作为主流的信息加密体制之一，与同样被广泛应用的非对称加密算法相比，具有**加解密速度快、安全性高、易于标准化**等优点，在**数据加密**、**认证**等方面发挥着非常重要的作用。

但是，当下对称密码的使用也有无法避免的**安全性**上缺点。首要的便是，使用对称密码要求提供一条安全的渠道使通讯双方在首次通讯时协商一个共同的密钥，即**密钥配送**问题。直接面对面协商不总是可行的，而密钥的运输过程很容易遭到攻击者的窃听，进而导致密码被破译。其次，对称密码的**密钥管理**也是相当困难的。假设要实现n个用户两两之间的保密通信，则每个用户都需要安全获取并保管与其他 n-1 个用户进行通信时的对称加密密钥。最后，对称密码算法一般不能提供信息完整性的鉴别，无法验证发送者和接受者的身份。

为了解决以上问题，发挥对称密码加解密速度更快、效率和安全性更高的优点，目前的主要方案是采用**混合密码系统**，即使用**对称密码加密信息提高处理速度，用公钥密码加密对称密码的密钥保护会话密钥**。在混合密码系统中，加入公钥密码以后，很轻松便弥补了对称密码的缺点。首先，关于密钥配送问题，使用公钥密码对会话密钥进行加密，即使加密过后的密钥和密文被窃听者获取，在私钥安全的前提下，窃听者也无法破译会话密钥，进而无法破译密文，获取信息。其次，对于密钥管理问题，数据的接收方无需再额外接收和保存会话密钥，只需要在接收到包含消息和会话密钥的密文以后，使用自己的私钥解密会话密钥，进而解密消息即可。并且由于公钥密码可以实现数字签名，对消息发送者的验证也可以轻松做到。

因此，对称密码学在安全中的具体应用，一般是**基于混合密码系统**的。例如，在https协议的数据传输阶段就用到了混合密码系统。其具体内容如下：

在证书验证阶段合法以后，本地生成随机数作为对称密码的密钥，用服务器端给出的公钥加密对称密码的密钥并将加密的密钥传输给服务端。在服务端接收到加密的对称密钥以后，用私钥解密该对称密码密钥，并用该会话密钥加密将要传输的数据。之后将该数据传输给客户端，客户端再用对称密码的密钥对接收到的密文进行解密。

在此过程中，由于混合密码的介入，使数据传输既保证了速度（对称密码加解密速度快），又保证了安全（对称密码自身安全性高，用于加密数据；公钥密码用于加密数据，保证对称密钥的安全性）。

综上，由于对称密码和公钥密码互相都存在一定的缺点并且可以通过一定的组合进行互补，集中各自的优点，因此在使用对称密码的安全应用中，一般辅以公钥密码保护会话密钥，保护数据安全。