加密学算法

1.对称密钥算法

2.非对称密钥算法

常用的加密算法

1.DES --Created by IGM，56bit key 对称加密算法

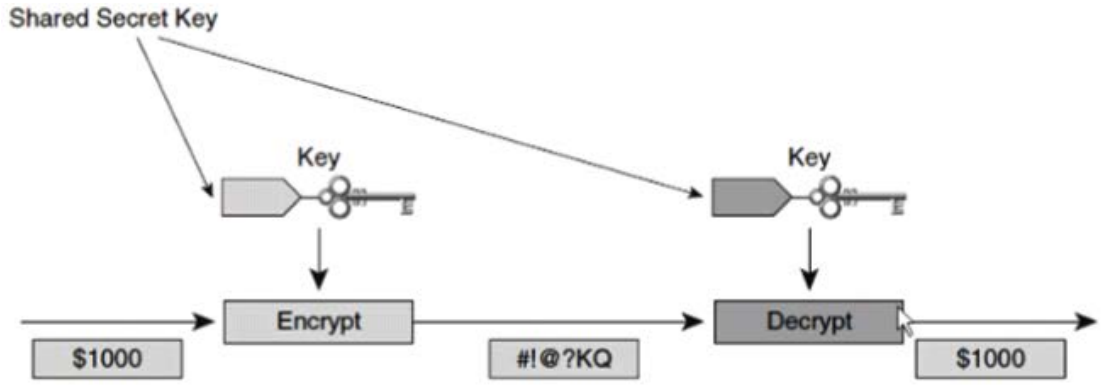
2.3DES --Uses three DES keys on each block of date to create 168bit keys 对称加密算法

3.AES --Newer，More efficient algorithm，128，192 and 256bit keys 对称加密算法

4.RSA --Used for “MISC” encryption，512，768，1024，2048bit or Lager 非对称加密算法

5.DH --Used commonly on VPN connections to allow secure transfer of shared secret keys（and helps generate shared secret keys）768，1024，1536 or Lager 非对称加密算法

对称密钥算法



注意：相同的密钥进行加解密

发送方和接收方使用相同的算法和相同的密钥，用某个密钥对明文数据进行加密，得到密文数据；接收方使用相同的算法和相同的密钥进行解密，得到明文。

优点：

1.速度快，比如：WIFI 使用的 WPA2 算法就是对称密钥算法

2.安全

3.紧凑，比如：一个 1500Byte 数据包，用 DES 加密之后，最多会增加 8Byte，通常是 4Byte

缺点：

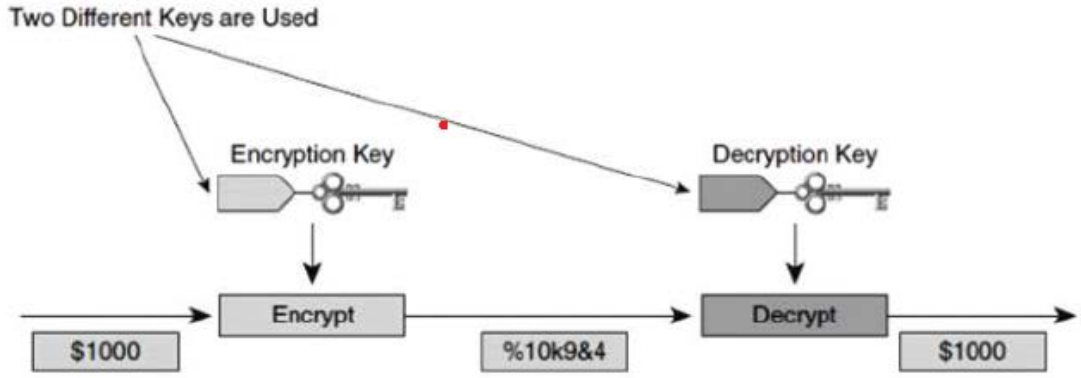
1.明文传输共享密钥，容易出现中途劫持和窃听的情况； 由于发起方和接收方使用同一个密钥，如何把这个密钥预先共享给另一方，这是一个安全问题

2.密钥的数量是以参与者数量平方进行增加的（指数增长）

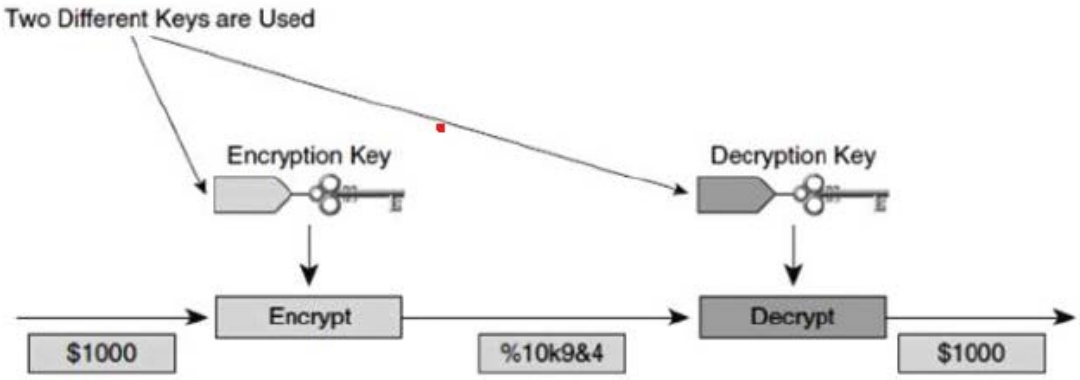
3.由于密钥的数量过多，管理和存储将会出现很大的问题
4.不支持数字签名和不可否认性

非对称密钥算法

场景一：用公钥加密，用私钥解密



场景二：用私钥加密，用公钥解密

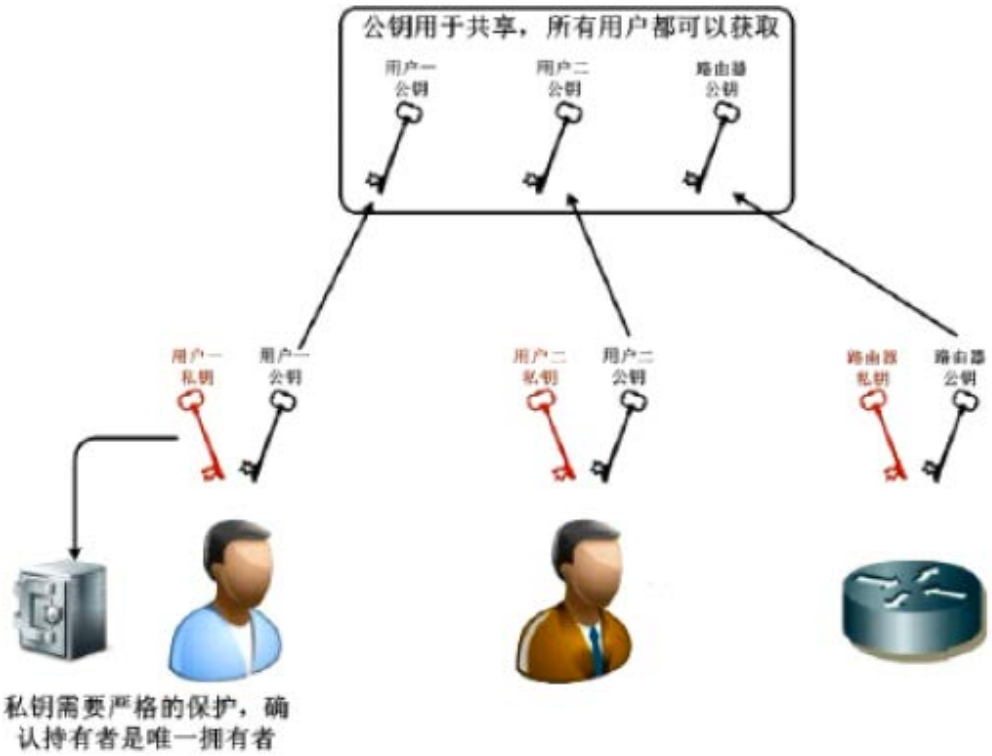


注意：不相同的密钥进行加解密

发送方和接收方使用不相同的密钥进行加密和解密。比如，发送方用公钥加密，接收方用私钥解密；发送方用私钥加密，接收方用公钥解密。

详解非对称密钥工作过程

用一个密钥（公钥）加密的数据只能用另一个密钥（私钥）解密

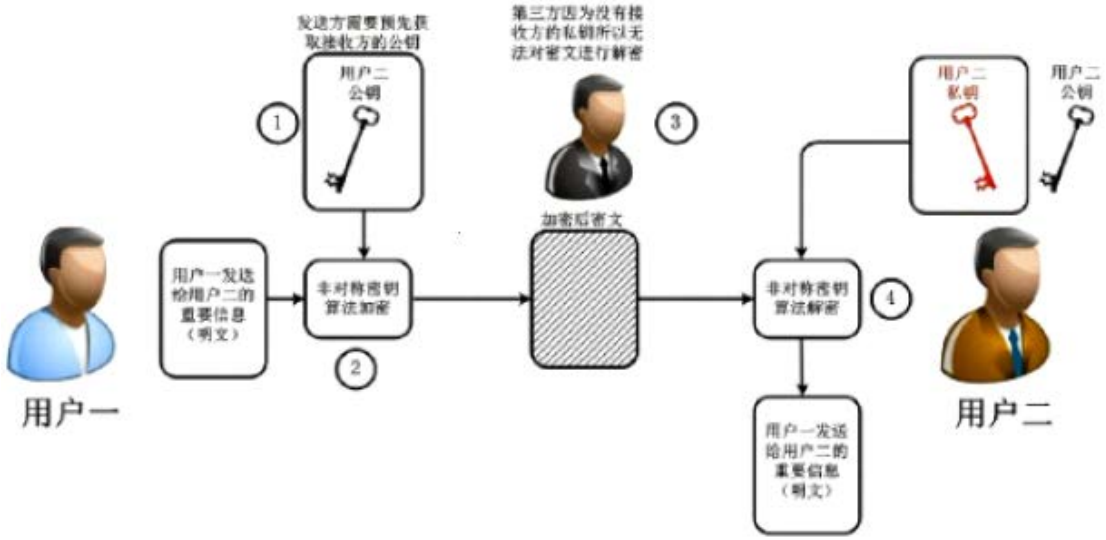


如上图所示，

1.通过非对称密钥算法产生一对密钥，一个叫公钥，一个叫私钥

2.私钥需要严格保护，公钥则可以公开，存放到公共服务器上，让其他人都可以获取。

举例说明



第一步：用户一先获取用户二的公钥

第二步：用户一把重要的明文数据信息用用户二的公钥进行加密，得到密文；穿越互联网的时候，第三方是无法解密，因为第三方无法获取用户二的私钥。

第三步：由于用户一使用用户二的公钥进行数据加密，所以用户二使用自己的私钥就可以解密，最终获取到明文数据。

优点

1.由于私钥是严格保密，不公开的；所以非对称密钥加密不必担心密钥被中途截取，安全性更高

2.密钥数量与参与者一致，不会成指数增长

3.不需要预先共享密钥，因为公钥是公开存放在服务器上，可供其他人下载，避免中途截取

4.可用于数字签名（加密散列）和密钥交换（加密密钥）

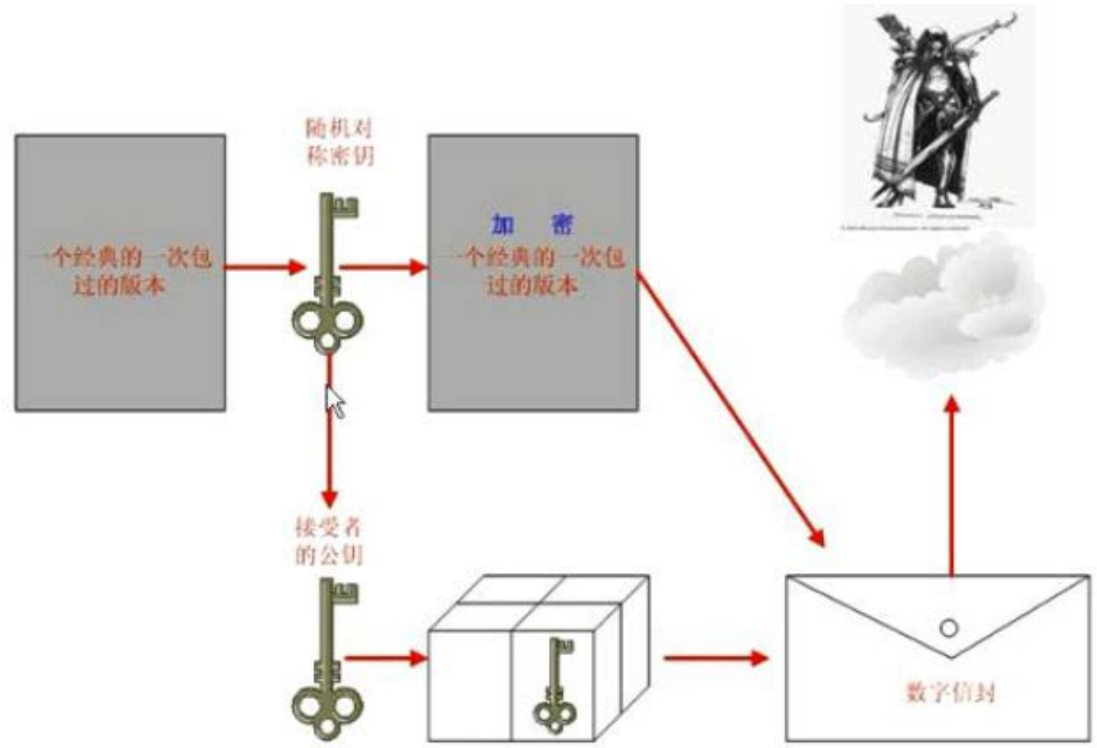
缺点

1.加密速度极慢，非对称密钥算法与对称密钥算法的速度相差近 1000 倍

2.加密后的密文会变长，比如：加密 1G 的明文数据将会变长 2G 的密文

一个简洁而优雅的解决方案

加密过程



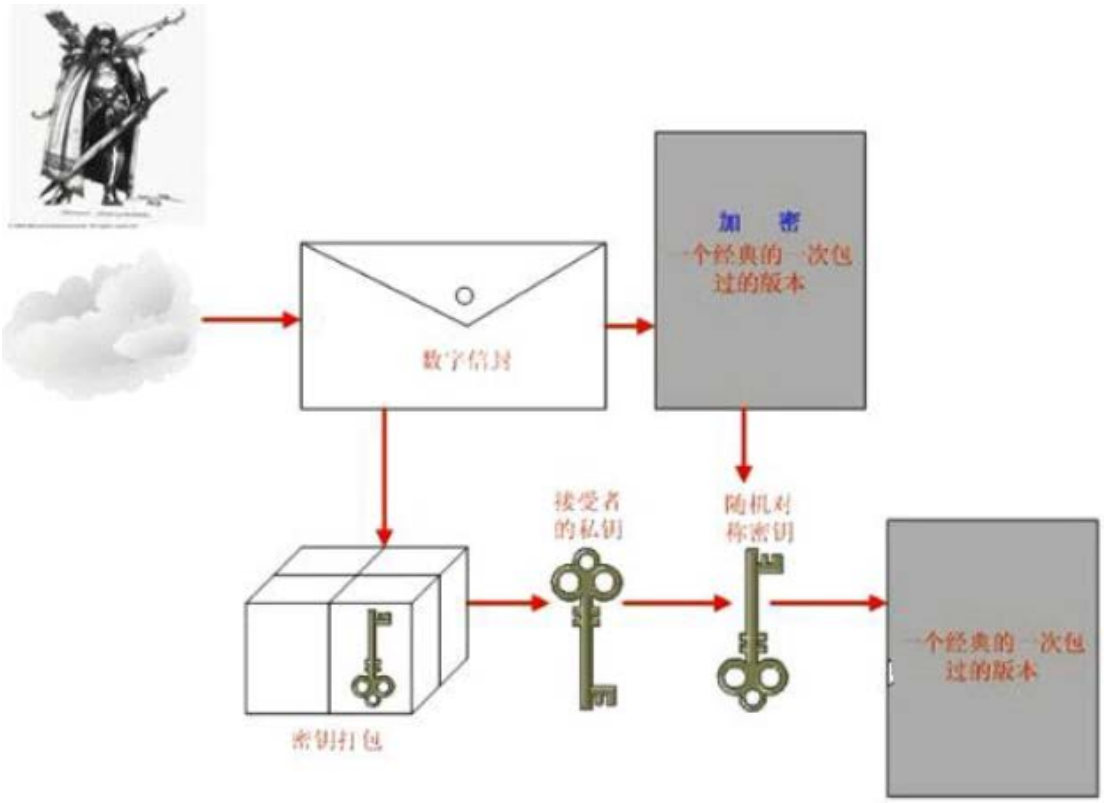
第一步：采取对称密钥算法来针对明文的资料进行加密，加密算法是又快又紧凑；

第二步：举例加密采用 DES 对称密钥算法来加密数据，对称密钥加密数据是需要一个密钥的，DES 加密数据是 56bit，密钥是发送方用 DES 进行加密，DES 密钥随机产生；

第三步：发送方获取接收方的公钥，用接收方的公钥对随机产生的密钥进行加密，得到一个密钥包；用非对称密钥算法加密这个密钥，虽然非对称加密算法很慢，但是只加密 56bit 是不需要花费太多时间；

第四步：得到一个密钥包之后，把密文资料和密文的密钥包封装到数据信封中，发送给接收方。

解密过程



第一步：接收方接收到数据信封后
第二步：针对密钥包使用接收方自己的私钥来解密；
第三步：得到一个明文 DES 用的 56bit 的随机密钥，相当于把密钥交换过来了
第四步：使用 56bit 的随机密钥和算法解密密文得到明文信息。

总结

用对称加密算法加密用户数据；
用非对称加密密钥，实现密钥交换

更多资讯，请关注微信公众号“广州华尔思网络实验室”动态信息。