数据安全及加密

一、简述 SSL 加密的过程用了哪些加密方法，为何这么作？

SSL 加密的过程之前有些过，此处不再赘述。

SSL 加密，在过程中实际使用了 对称加密 和 非对称加密 的结合。

主要的考虑是先使用 非对称加密 进行连接，这样做是为了避免中间人攻击秘钥被劫持，但是 非对称加密的效率比较低。所以一旦建立了安全的连接之后，就可以使用轻量的 对称加密。

二、RSA 非对称加密

对称加密[算法]在加密和解密时使用的是同一个秘钥；而[非对称加密算法]需要两个[密钥]来进行加密和解密，这两个秘钥是[公开密钥]（public key，简称公钥）和私有密钥（private key，简称私钥）。

RSA 加密

与对称加密[算法]不同，[非对称加密算法]需要两个[密钥]：[公开密钥]（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的[密钥]，所以这种算法叫作[非对称加密算法]。

RSA 加密原理

RSA 是常用的加密模式，其加密原理可用以下的例子进行简要的论述。

随机取两个质数

```
P = 61;
q = 53;
N = P * Q = 3233;
// E是1-n之间的一个随机的质数
E = 17;

// D是通过一系列数学运算得出的一个数字，
// 运算方法后续会附上阮一峰老师的两篇文章链接
// (N,D)(N,E)要满足可以互相解值运算
// 假如(N,D)是公钥，(N,E)是私钥
// 满足私钥加密，公钥解密或者反过来公钥加密，私钥解密
// 也要满足只知道(N,D)就算知道N,E,也很难把N分解成这个大的整数进行因数分解。
// 因数分解只能使用最大的质数，N越大，相应的D就越安全
// 当 N 大到1024位或者2048位时，以目前的技术破解几乎不可能，所以很安全
```