网络与信息安全课内实验三

对称、非对称加解密

一．实验目的

1. 加深对非对称，对称加解密算法、散列函数的理解。

2. 了解常用加密工具包以及相关库函数的使用。

3. 了解ssl协议

二．实验原理

1. 对称加密 采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种 加密方法称为对称加密，也称为单密钥加密。在对称加密算法中常用的算法有：DES、 3DES、TDEA、Blowfish、RC2、RC4、RC5、IDEA、SKIPJACK 等。 对称加密算法的缺点是在数据传送前，发送方和接收方必须商定好秘钥，然后使双 方都能保存好秘钥。其次如果一方的秘钥被泄露，那么加密信息也就不安全了。另外， 每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一秘钥，这会使得收、 发双方所拥有的钥匙数量巨大，密钥管理成为双方的负担。

2. 非对称加密 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。 非对称加 密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密 钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲 方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。

3. 散列函数 Hash，一般翻译做"散列"，也有直接音译为"哈希"的，就是把任意长度的输入（又 叫做预映射， pre-image），通过散列算法，变换成固定长度的输出，该输出就是散列值。 这种转换是一种压缩映射，也就是，散列值的空间通常远小于输入的空间，不同的输入 可能会散列成相同的输出，而不可能从散列值来唯一的确定输入值。简单的说就是一种 将任意长度的消息压缩到某一固定长度的消息摘要的函数。

三．实验步骤

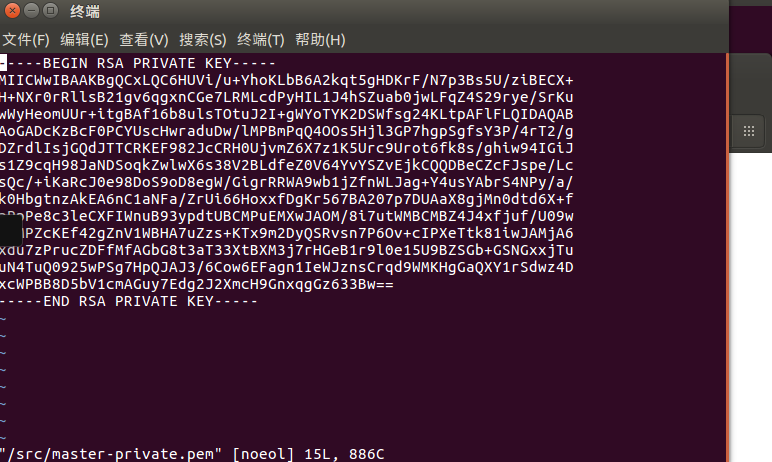
1. 对称加密算法的字符串的加解密

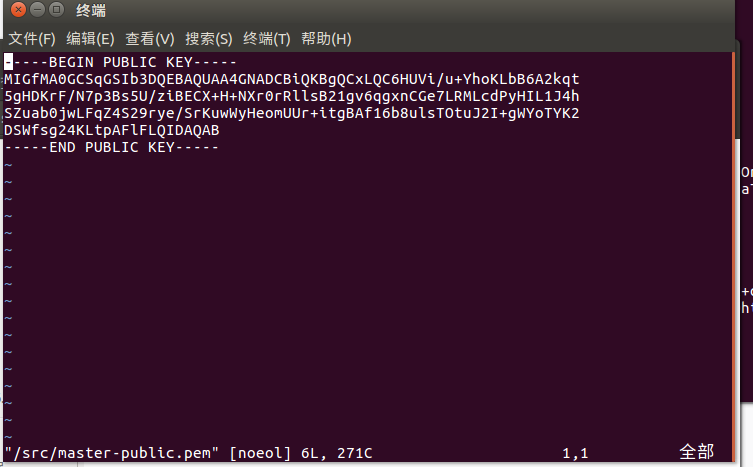
使用AES算法对字符串进行加密



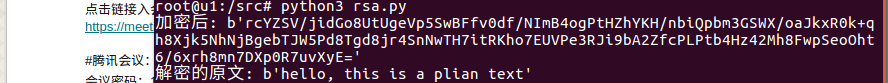
2. 使用RSA的加解密

1）生成公私钥



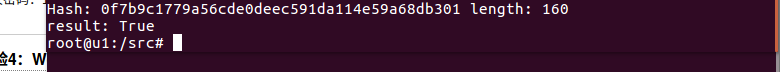


2）使用公钥加密，并使用私钥解密



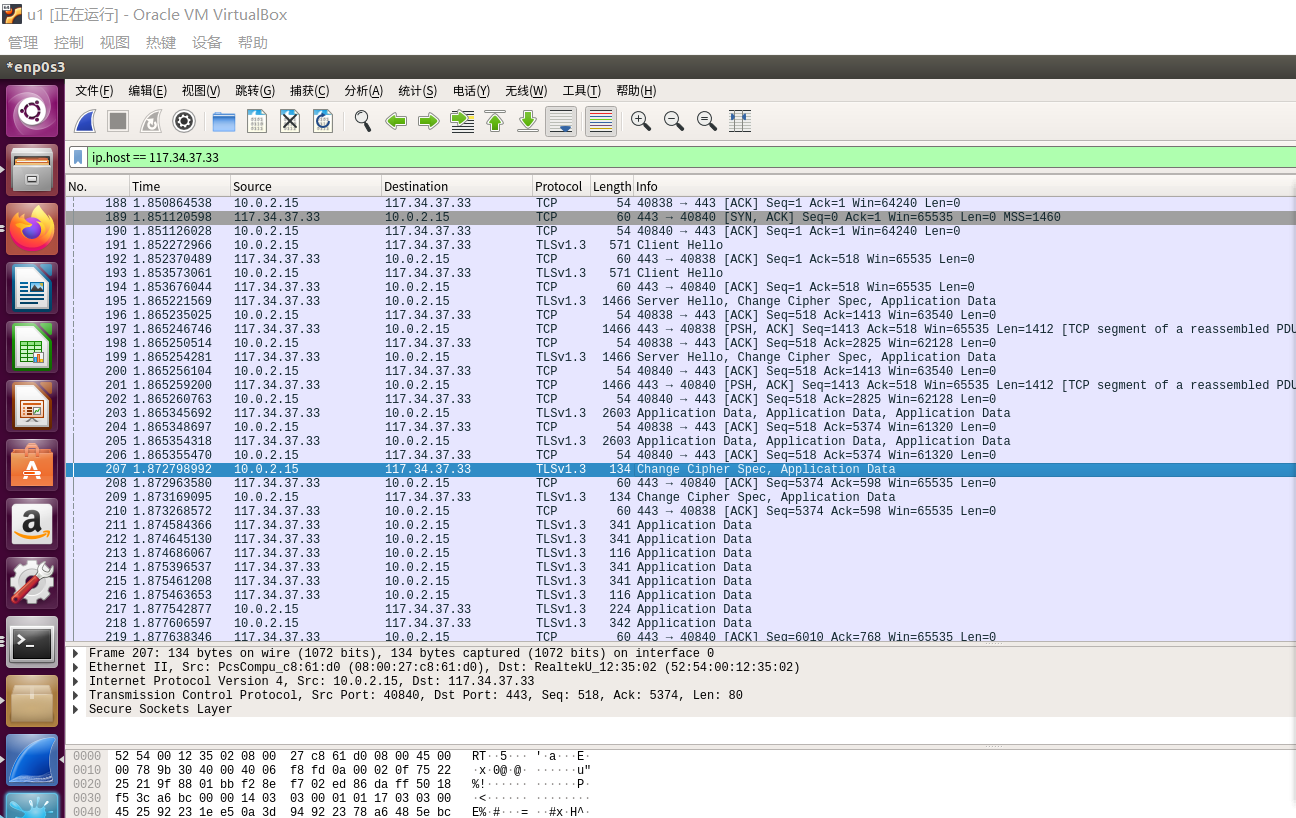
3. 数字签名

尝试使用RSA进行数字签名



4. 抓包观察 ssl 协议通信握手过程

访问<https://www.baidu.com/>，并使用wireshark抓包



四．思考题

1. 回答AES加密中iv变量的作用。

答：使用随机数产生的初始化向量才能达到语义安全，并让攻击者难以对同一把密钥的密文进行破解。初始化向量的值依密码算法而不同。最基本的要求是唯一性，也就是说同一把密钥不重复使用同一个初始化向量。

1. 思考问题：RSA【公钥加密，私钥解密】和【私钥加密，公钥解密】算法一样吗？为什么？

答：不一样。前者属于对称加密，后者属于非对称加密。RAS的公钥加密和私钥解密用的同一密钥。

1. 详细分析ssl 协议通信握手过程。

答：1.客户端发送随机数s1,SSL版本号以及可选的加密算法给服务器B。

2.服务器B从可选的加密算法中选择其中一种作为服务器支持的加密算法(暂且称其为m),并且产生一个随机数s2。

服务器将m、s2和一份包含服务器B的RSA公钥的数字证书发送给客户端；该证书还包含了用于认证目的的服务器标识。

3.客户端A使用该证书的认证机构CA公开发布的RSA公钥对该证书进行验证(如果认证机构不靠谱，那就很难受了),同时客户端A又产生一个随机数s3（产生这么多随机数我也很绝望），其实s3有一个专门名称，叫做pre\_master\_secret。客户端将使用服务器B发送过来的服务器RSA密钥匙(就是存放在数字证书中的那个密钥)对s3进行加密后，得到的内容message,将其发送给B。

4.B用自己的私钥将message解密，此时，客户端和服务器都拥有s1,s2,s3的内容，它们将分别利用这三者的内容独立计算出共享的对称会话密钥(至于怎么计算的，可自行搜索DH密钥交换算法了解，当然我自己也准备写一篇文章来介绍)。本来有了对称密钥，就可以进行通信了，但是为了防止握手本身遭受篡改，还需要进行以下两步检验：

5.客户端将所有握手消息的MAC值发送给服务器；

6.服务器将所有握手消息的MAC值发送给客户端；