加密类型和算法

裸奔协议： http ftp smtp telent

机密性 数据完整性 身份验证

plaintext ---转换规则 --- ciphertext

ciphertext ---转换规则--- plaintext

转换算法（数学原理）： 秘钥（自己换）

对称加密：

秘钥是相同的，计算速度非常快，安全性完全依赖于秘钥，一但通信双方数量增加，秘钥数量也要增加，秘钥管理也是很头痛的事情。

单向加密算法

提取数据特征码（指纹）附加在明文后面，对方接受到后采用相同的加密算法，对信息提取特征码，进行对比就知道信息有没有被篡改。

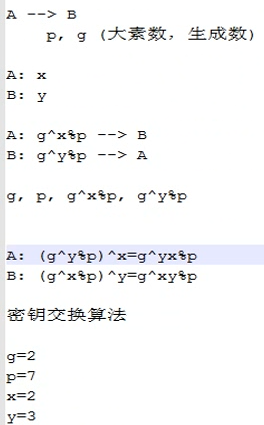
1. 输入一样，输出必然相同
2. 雪崩效应，微小的改变会引起结果的巨大改变
3. 定长输出，无论原始数据多大，结果大小相同
4. 不可逆，无法根据特征码还原原来的数据

不能应对中间人攻击，不能保证机密性，中间人获取明文后重新生成特征码，发送给接收方

将特征码加密

协商生成密码： 秘钥交换（Internate key exchange ,IKE），需要互联网协议支撑

Diffie-Hellman协议就是著名的秘钥交换算法，离散对数原理



公钥加密算法：非对称加密:

密钥对：

公钥：p 从私钥总提取

私钥：s

发送方用自己的私钥加密能保证身份验证，私钥只有自己才有，确定身份

私钥加密并不能保证数据的机密性，任何持有公钥都可以解密

发送方用对方的公钥加密能保证数据的机密性，公钥加密只有私钥解密。

有机密性无身份验证，有身份验证无机密性。

我想跟谁通信，就用谁的公钥加密。谁要和我通信，他就用我的公钥加密。反正我就记住我的一对秘钥，解决了对称加密的密码管理的问题。

公钥加密算法很少用来加密数据，密码太长，速度太慢，比对称加密要慢上3个数量级。

通常用来进行身份验证，