### 密码编译工具

对称加密

对称加密的五个基本成分

|  |  |
| --- | --- |
| 明文 | 原始的消息和数据 |
| 加密算法 | 对明文进行各种代换和变换 |
| 秘密秘钥 | 算法所用的特定的代换和变化依赖于秘钥 |
| 密文 | 算法的输出，看起来完全随机，依赖于算法和秘钥 |
| 解密算法 | 加密算法的逆运算，输入密文和秘钥可以恢复明文 |

对称分组加密算法 ： 一次输入一组元素，每个输入分组产生一个输出分组

流密码 ：持续的处理输入元素，每次产生一个元素的输出

消息认证和散列函数

1利用对称加密实现认证 ：纠错码和序号 时间戳

2.无需加密的消息认证：消息认证码（双方用相同的秘钥和算法处理得到相同的消息认证码）

对散列函数的要求：

1. H可以应用于任意大小的数据块
2. H产生固定长度的输出
3. 对于给定的x H（x）容易计算
4. 对于任意的散列码 散列函数是单向的 或是抗原象
5. 弱抗碰撞性 意味着相同的不同的x不会产生相同的散列码
6. 强抗碰撞性 阻止一个实体伪造另一个实体已经签名的信息

2.3 公钥加密

|  |  |
| --- | --- |
| 明文 | 算法的输入 |
| 加密算法 | 对明文进行各种变化 |
| 公钥和私钥 | 一个用于加密一个用于解密 |
| 密文 | 算法的输出 |
| 解密算法 | 接受密文和秘钥 |

机制 ：每个用户产生一对密钥，将其中一个密钥放在公共寄存器中作为公钥，另一个则为秘钥，若给tag发消息，则使用tag的公钥加密，tag接收后用与之配对的私钥进行解密。