蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

哈希函数定义与特性

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解密码学基础知识
- 了解哈希函数定义
- 了解哈希函数特性

01 密码学概述

密码学简介

密码学主要功能

密码学术语

密码学简介

- 密码学是研究编制密码和破译密码的技术科学。
- 密码学是信息安全等相关议题，如认证、访问控制的核心。
- 密码学的首要目的是隐藏信息的涵义，并不是隐藏信息的存在。
- 密码学促进了计算机科学，特别是在于电脑与网络安全所使用的技术。
- 密码学已被应用在日常生活。

密码学主要功能

密码学主要功能是机密性，鉴别，报文完整性和不可否认性

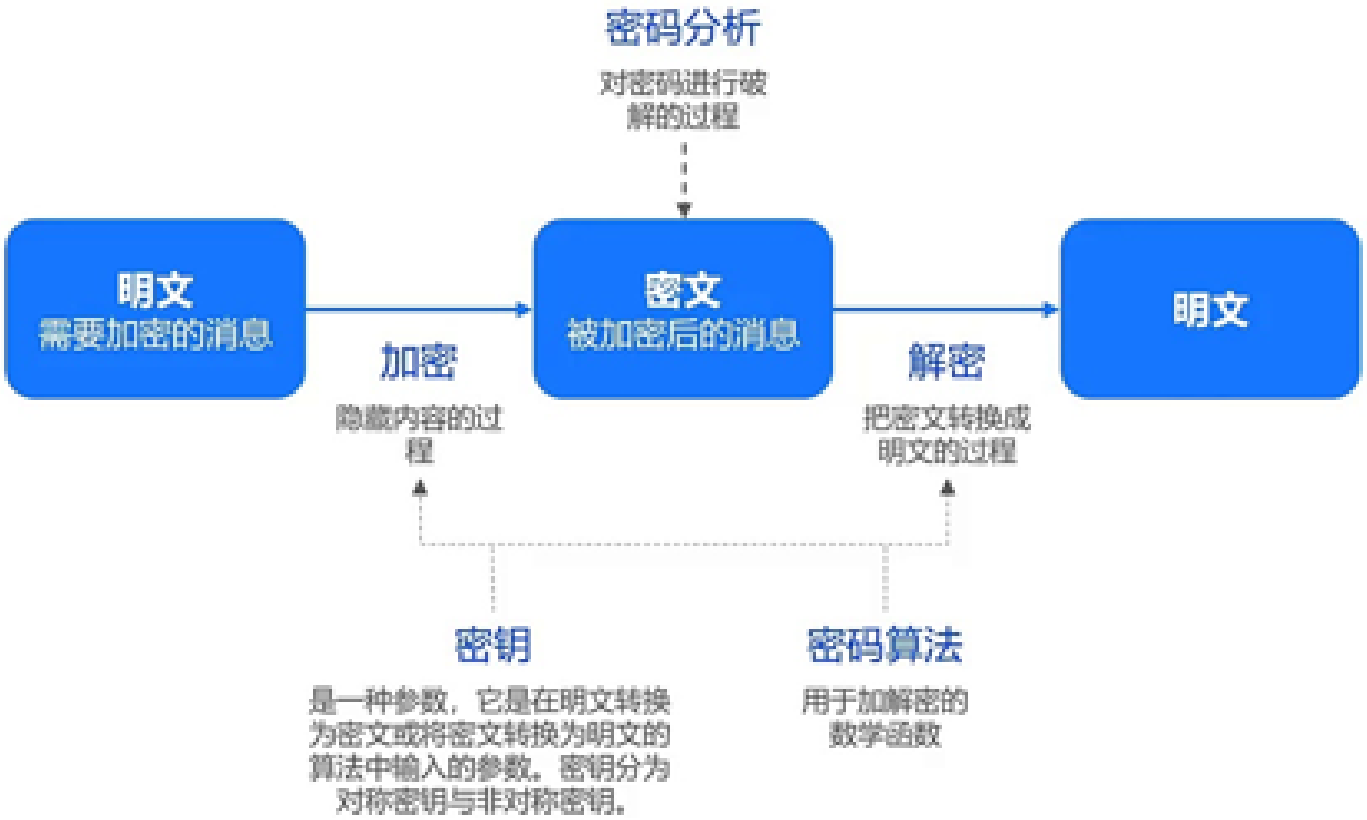
机密性
——保密信息不会透露给非授权用户或实体

鉴别
——一个消息的来源和消息本身被正确的标识，同时确保该标识没有被伪造

报文完整性
——信息在生成，传输，存储和使用过程中发生的人为或非人为的非授权篡改均可以被检测到

不可否认性
——用户无法在事后否认曾经进行信息的生成，签发，接收行为

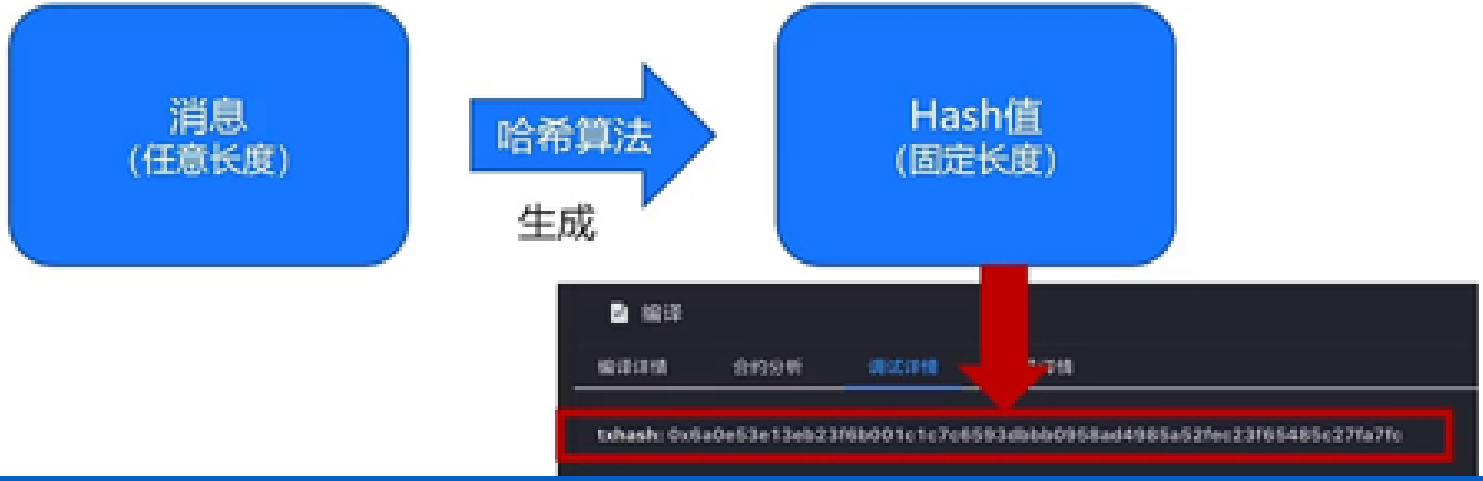
密码学术语


密码分析
对密码进行破解的过程
明文
需要加密的消息
加密
隐藏内容的过程
密文
被加密后的消息
解密
把密文转换成明文的过程
明文
密钥
是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥分为对称密钥与非对称密钥。
密码算法
用于加解密的数学函数

什么是哈希函数

哈希函数的定义

- Hash，一般翻译做散列、杂凑，或音译为哈希，是把任意长度的输入通过哈希算法变换成固定长度的输出，该输出就是散列值。
- 能够实现该功能的算法叫做哈希算法，能够实现哈希算法要求的函数叫做哈希函数。
- 哈希函数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。



哈希算法特点和常用哈希算法

哈希算法特点

- 单向性
- 确定性
- 不可逆性
- 固定长度
- 抗碰撞性

常用哈希算法

- MD5 信息摘要算法
- SHA-1 安全散列算法1
- SHA-256 安全散列算法256

哈希函数作用

哈希函数的作用是防止数据篡改，软件保护和口令保护

防止数据篡改

原始数据和经过哈希算法得到的数据一块发送给对方，对方收到数据之后，对数据使用相同的哈希算法进行计算，如果得到的哈希值和对方发过来的相同，那么就说明数据没有经过篡改。

软件保护

对外发布软件时，同时使用哈希函数计算出软件的哈希值，与软件一起发布，防止用户下载假冒软件。

口令保护

账户系统的口令通过哈希函数处理后，再存储于服务器上，使得口令只对用户自己可知。

总结

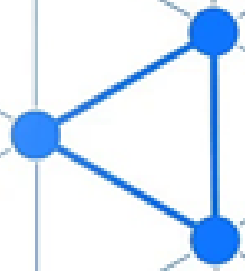
■ 密码学

- 密码学主要功能是机密性，鉴别，报文完整性和不可否认性

■ 哈希函数

- 哈希函数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
- 哈希函数的作用是防止数据篡改，软件保护和口令保护

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN