蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

# 对称加密算法上

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

**课程目标**

- 了解对称加密的相关知识
- 了解DES和AES

# 对称加密体制

## 概述

如果一个密码体制的加密密钥和解密密钥相同，或者虽然不相同，但是由其中的任意一个可以很容易地推导出另一个，则该密码体制便称为对称密钥加密体制。

## 特点

- 加密密钥和解密密钥相同，或本质上相同
- 密钥必须严格保密

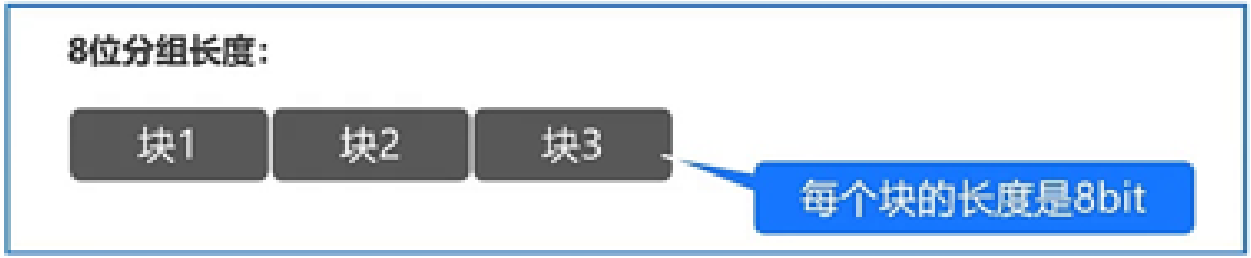
## 常用算法

- DES
- 3-DES
- IDEA
- AES
- ……

# 前置知识·分组和替代

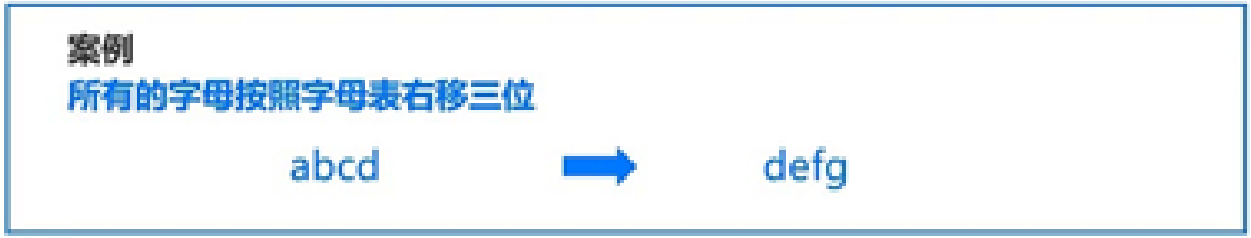
**分组**

把很长的消息分成一组一组的固定长度的数据块




**替代**

用一个字符替代另外一个字符



# DES算法的由来和技术特点

## DES算法的由来

DES加密算法是1972年美国IBM公司研制的对称密码体制加密算法，
又被称为美国数据加密标准。

## DES算法特点

- 分组加密算法：明文和密文为64位分组长度。
- 对称算法：加密和解密除密钥编排不同外，使用统一算法。
- DES的安全性不依赖于算法的保密，安全性仅以加密密钥的保密为基础。
- 密钥可为任意56位数，具有复杂性，使得破译的开销超过可能获得的利益。
- 采用替代和置换的组合，共16轮 。

# DES算法的基本工作原理-加密流程

## 加密流程

用56位的密钥对64位长的数据块进行16轮加密处理，由此得到64位长的密文。

在加密过程中，会对56位密钥进行置换，生成不同的16个子密钥，依次用在16轮的加密处理中。

# AES算法和特点

## AES算法

- AES是密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。
- AES是一个新的可以用于保护电子数据的加密算法。

## AES算法特点

- 密钥长度（128位，192位，256位）是可变的，明文密文长度固定为128位
- AES是面向字节的运算
- AES加密算法与解密算法不一致

| | 密钥长度（bit） | 分组长度（bit） | 加密轮数 |
|---|---|---|---|
| AES-128 | 128 | 128 | 10 |
| AES-192 | 192 | 128 | 12 |
| AES-256 | 256 | 128 | 14 |

# AES算法和特点

## AES算法

- AES是密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。
- AES是一个新的可以用于保护电子数据的加密算法。

## AES算法特点

- 密钥长度（128位，192位，256位）是可变的，明文密文长度固定为128位
- AES是面向字节的运算
- AES加密算法与解密算法不一致

| | 密钥长度（bit） | 分组长度（bit） | 加密轮数 |
|---|---|---|---|
| AES-128 | 128 | 128 | 10 |
| AES-192 | 192 | 128 | 12 |
| AES-256 | 256 | 128 | 14 |

# AES算法的基本工作原理

- **AES加密流程(以AES-128为例)**

1.将128位的密钥扩展至加密过程中需要的10轮轮函数密钥。

2.对明文进行分组，每组长度都是128位，然后一组一组的进行加密。

3.加密过程中会执行一个包含各种基本运算的轮函数，轮函数加密使用密钥扩展的轮函数密钥。

4.将加密后的密文拼凑起来，得到最终的完整密文。

- **AES解密流程(以AES-128为例)**

AES解密算法与加密不同，基本运算中除了AddRoundKey（轮密钥加）不变外，其余的都需要进行逆变换。

# 总结

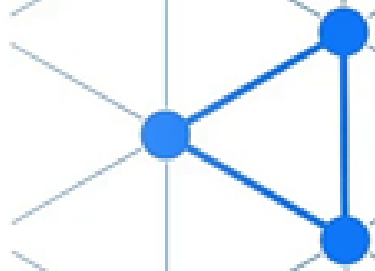
## ■ 对称加密体制

- 加解密的密钥相同或者本质上相同的加密体制叫做对称加密体制

## ■ DES和AES

- DES是用56位的密钥对64位长的数据块进行16轮加密处理，由此得到64位长的密文
- AES根据密钥长度不同，加密的轮数也不一样
- DES加解密可以使用同一算法，AES不能

# 谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN