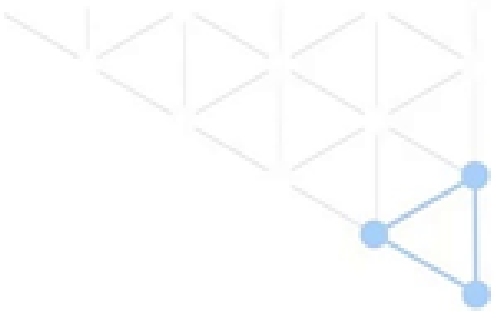
蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

非对称加密

- 蚂蚁链《区块链系统开发与应用》A认证系列课程



课程目标

- 了解非对称加密的相关知识
- 了解RSA和ECC

非对称加密

如果一个密码体制的加密/ 解密操作分别使用两个不同的密钥，并且不可能由加密密钥推导出解密密钥，则该密码体制称为非对称加密体制。

其特点为：

- 加密密钥和解密密钥不同，并且难以互推
- 有一个密钥是公开的，即公钥，而另一个密钥是保密的，即私钥

□ 常用的非对称加密算法有RSA、ECC 等。

02 RSA

RSA密码体制

RSA算法特点

公钥加密算法（RSA）

RSA算法简单的原理

- RSA算法基于一个非常简单的数论事实：两个素数（质数）相乘得到一个大数很容易，但是由一个大数分解为两个素数（质数）相乘却非常难。

- RSA算法是一种非对称的算法，该算法需要一对密钥，使用其中一个加密另一个就可以进行解密。

RSA算法的特点

安全性依赖于大数的质因子分解

破解密钥的成本远远大于收益

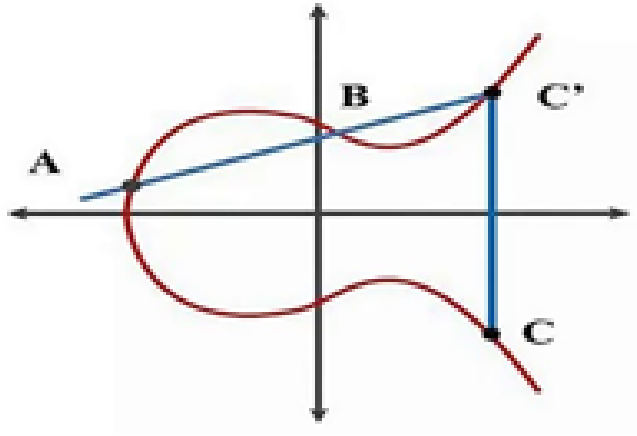
产生密钥很麻烦，需要花费的时间很长

只能加密少量数据，大量数据加密还需对称加密

椭圆曲线密码体制（ECC）

Neal Koblitz和Victor Miller在 1985年分别提出了椭圆曲线密码体制(ECC)，它是迄今为止被实践证明安全有效的三类公钥密码体制之一。

- ECC的安全性基于椭圆曲线离散对数问题的难解性
- ECC密钥长度大大减少
- 1998年被ISO/IEC定为数字签名标准， 2000年2月定为IEEE标准。



区块链中主要使用非对称加密的ECC椭圆曲线算法。

椭圆曲线公钥系统的优点

椭圆曲线公钥系统是代替RSA的强有力的竞争者，有以下的优点。

安全性能更高

如：256位ECC与3072位RSA有相同的安全强度

计算量小，处理速度快

在私钥的处理速度上（解密和签名），ECC远比RSA、DSA快得多

存储空间占用小

ECC的密钥尺寸和系统参数与RSA、DSA相比要小得多，所以占用的存储空间小得多

总结

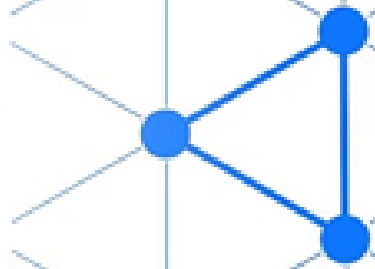
■ 非对称加密体制

- 加解密的密钥不相同并且无法互推的加密体制叫做非对称加密体制

■ RSA和ECC

- RSA是基于大整数分解类的加密体制，ECC是基于椭圆曲线类的加密体制
- ECC在加密速度,安全性和空间占用方面都优于RSA

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN