# 密码技术

本文主要介绍为了保证信息机密性、完整性和可用性（CIA三要素）而采用的密码技术。

通过加密技术可以保证信息的机密性。加密技术从密钥类型上来分可以分为对称密码和公钥密码，从密码算法处理数据的模式上来分可以分组密码和流密码。这里主要介绍对称密码、公钥密码和分组密码模式（传输大量数据时需要用到的分组加密模式）。

通过认证技术中的消息认证码和数字签名技术可以保证信息的完整性。而贯穿其中的单向散列函数也是我们讲解的重点。通过认证技术中的证书可以保证信息的可用性。

而最后介绍的随机数在以上的各种技术中一般担当随机密钥的角色。因此密钥的不可预测性也显得至关重要。

## 1、对称密码

对称密码中加密和解密时都是使用的同一个密钥（密钥是对称的），因此获得了对称密码的称

号。这里我们主要介绍三种对称密码算法：一次性密码本、DES、AES。

### 1.1、一次性密码本

一次性密码本属于流密码，并被称为绝对不会被破译的密码（即便使用暴力破解也无法破译），我们可以带着这个结论去看下面的介绍。

#### 数学原理

一次性密码本算法的基本运算就是异或运算，其中规定了密钥的长度要和明文的长度一致，因此加密后的密文与明文长度是一致的。

|  |  |
| --- | --- |
| **加密** | **解密** |
| 密文 = 明文⊕密钥 | 明文 = 密文⊕密钥 |

#### 不可破译性

那么为什么一次性密码本是不会被破译的呢？试想一下我们使用暴力破解去破解密钥的过程。首先，密钥长度和明文长度一致而明文长度和密文长度一致，这就可以通过密文长度确定密钥空间。接着，我们开始使用每一个可能的密钥去解密，这时会发现每一个密钥都可以解密出对应的明文，但是我们却无法确认哪一个明文是正确的明文，这也就造成了一次性密码本的不可破译特性。

#### 算法分析

|  |  |
| --- | --- |
| **优点** | **缺点** |
| 1.无法破译，安全性极高 | 1.存在密钥配送问题 |
| 2.效率高 | 2.密钥保存代价高 |
|  | 3.密钥不可重用 |
|  | 4.密钥同步易出错 |
|  | 5.密钥生成难度高 |

该算法的核心运算是异或运算，这就使得一次性密码本的效率非常高；而由于其独特的不可破译特性，也让一次性密码本有了非常高的安全性。

但是一次性密码本却很少被使用，这又是为什么呢？算法本身已经证明是无法破译的，那么安全的关键就在于密钥的安全性，那么应该是密钥的安全性方面的问题导致了一次性密码本的不实用。

首先，存在密钥配送问题，要保证密钥不泄露就必须保证具有一个合理的方式来让双方商议密钥，这个在后续的介绍中可以了解到公钥加密、Diffie-Hellman密钥交换等算法来解决。

其次，存在密钥保存问题，密钥的长度要与明文的长度一致，那么保存明文变成了保存长度一致的密钥，并没有从本质上解决问题。

接着，由于一次性密码本每次通信都要用到新的密钥（这也是一次性的意义），导致了密钥不可重用的局限性。

然后，在通信过程当中需要传输与明文长度一致的密钥，那么当明文很长时，密钥对应的也会很长，这就大大增加了密钥在同步过程当中出错的概率，而一旦密钥出错，也就无法加密了。

最后，一次性密码本中需要生成大量的随机数，而这里的随机数并不是指程序生成的伪随机数，而必须是无重现的真随机数。

### 1.2、DES

DES属于分组密码，并且每次只能加密64比特的数据，如果要加密长明文就需要对DES机密进行迭代。DES加密算法如今已经可以在短时间内破译了，因此除了兼容旧系统，都不用DES加密。

#### 数学原理

DES的基本结构时Feistel网络，在Feistel网络中加密的各个步骤称为轮，整个加密过程就是若干次轮的循环，而DES是一种16轮的循环的Feistel网络。下面以三轮的循环的Feistel网络为例介绍DES。

### 1.3、AES

### 1.4、总结

## 2、分组密码模式

## 3、公钥密码

## 4、单向散列函数

## 5、消息认证码

## 6、数字签名

## 7、证书

## 8、随机数

## 9、总结