

编码&哈希摘要&对称加密

2019年3月11日 21:21

■ 编码与解码

编码是将信息从一种格式（人能识别）转换为另一种形式（计算机能识别）的过程，反之成为解码。

字符集与字符编码 <<http://www.cnblogs.com/skynet/archive/2011/05/03/2035105.html>>

理解字符集和编码，常见字符集名称：ASCII、GB2312、BIG5、GB18030 和 Unicode 字符集。

```
int unicode = char.Parse("零");  
var unicodeCodeString = Convert.ToString(unicode, 2);
```

微软提供的主要类：System.Text.Encoding

```
var bytes = BitConverter.GetBytes(unicode);  
UTF32Encoding encoding = new UTF32Encoding();  
var str = encoding.GetString(bytes);
```

关于 Base64 编码

Base64编码原理 <<https://www.jianshu.com/p/8aa883943ab3>>

```
byte[] bytes = Encoding.Default.GetBytes(str);  
string baseString = Convert.ToBase64String(bytes);  
  
byte[] bytes = Convert.FromBase64String(baseString);  
var str = Encoding.Default.GetString(bytes);
```

■ 哈希散列摘要算法

Hash，一般翻译做散列，音译为哈希，是把任意长度的输入通过散列算法变换成固定长度的输出，该输出就是散列值。简单的说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算法或者函数，有时也叫摘要算法。

目前主流的 Hash 算法有：MD4、MD5 和 SHA 系列。

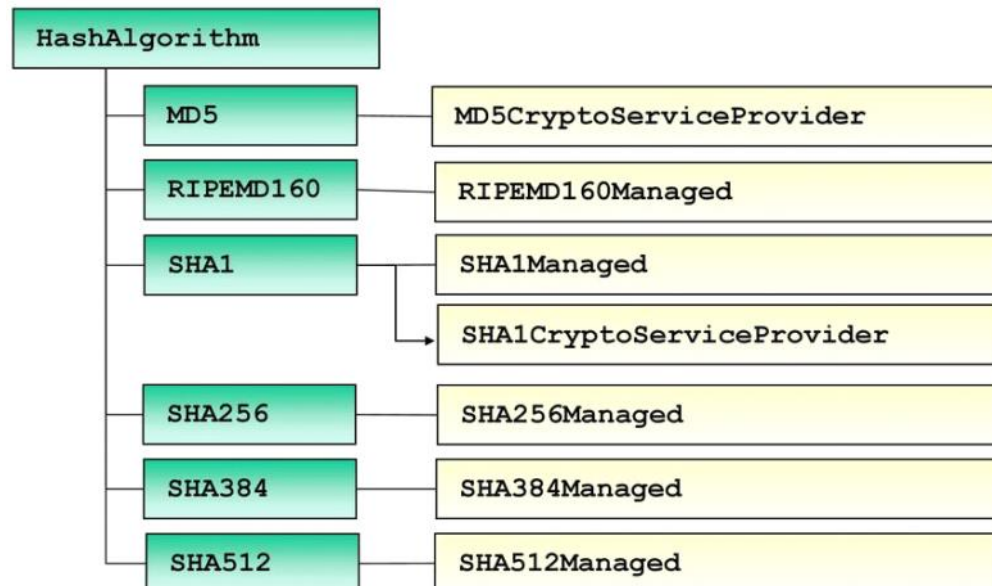
什么是Hash算法 <<https://www.jianshu.com/p/bba9b61b80e7>>

SHA家族有5个算法：SHA-1，SHA-224，SHA-256，SHA-384 和 SHA-512，其中后 4 者总称 SHA2 算法。

用途：文件校验、数字签名 和 鉴权协议。

浅谈hash一致性算法 <<https://www.jianshu.com/p/6f13156573f4>>

微软实现来自 <<https://github.com/dotnet/corefx/tree/master/src/System.Security.Cryptography.Algorithms>>



```
public byte[] ComputeHash(byte[] buffer)

string strContent = "www.xcode.me;video.xcode.me";

byte[] bytes = Encoding.Default.GetBytes(strContent);

//var sha1 = new
System.Security.Cryptography.SHA1CryptoServiceProvider();

var sha1 = System.Security.Cryptography.SHA1.Create();

byte[] result = sha1.ComputeHash(bytes);

string sha1HashString = BitConverter.ToString(result);
```

HMAC 是具密钥的哈希算法，以一个密钥和一个消息为输入，生成摘要作为输出。

消息 + 密钥 + 算法 ==》输出摘要

```
string strText = "This is .net core website";

string strKey = "www.xcode.me";

HMACSHA1 hmacsha1 = new HMACSHA1(Encoding.UTF8.GetBytes(strKey));

byte[] bytes = hmacsha1.ComputeHash(Encoding.UTF8.GetBytes(strText));

string hmacSha1String= BitConverter.ToString(bytes);

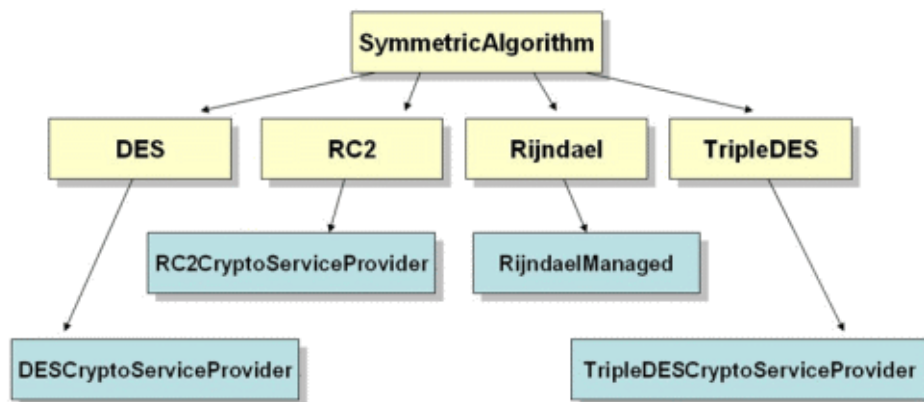
string hmacSha1BaseString = Convert.ToBase64String(bytes);
```

校验摘要：就是将原文进行同样的算法后比较摘要的过程。

■ 对称加密算法

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

常见的对称加解密算法：Aes、RC2、DES、TripleDES 和 Rijndael 算法。



[TripleDESCryptoServiceProvider使用示例](#)

来自简书的TripleDES加密示例 <<https://www.jianshu.com/p/0781a6f21305>>