## Windows下的bat文件的@echo off 作用？

## RSA算法

### 简介

RSA公开密钥密码体制是一种使用不同的加密密钥与解密密钥，“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

在公开密码体制中，加密密钥PK是公开信息，而解密密钥SK是需要保密的。加密算法E和解密算法D也都是公开的。虽然解密密钥SK是由公开密钥PK决定的，但却不能根据PK计算出SK。

正是基于这种理论，1978年出现了著名的RSA算法，它通常是先生成一对RSA密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA密钥至少为500位长。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的DES或IDEA对话密钥加密，然后使用RSA密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

### 算法原理

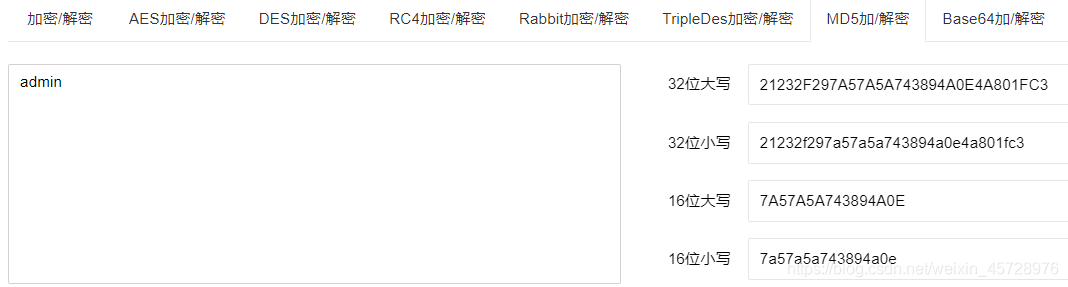
RSA公开密钥密码体制的原理是:根据数论，寻找两个大素数比较简单，而将他们的乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

## 加密编码类型的密文特征分析

### MD5、sha1、HMAC算法、NTLM等相似加密类型

#### MD5——示例21232F297A57A5A743894A0E4A801FC3

**一般MD5值是32位由数字“0-9”和字母“a-f”所组成的字符串**，如图。如果出现这个范围以外的字符说明这可能是个错误的md5值，就没必要再拿去解密了。16位值是取的是8~24位。



**md5的三个特征：**

1. **确定性**：一个原始数据的MD5值是唯一的，同一个原始数据不可能会计算出多个不同的MD5值。
2. **碰撞性**：原始数据与其MD5值并不是一一对应的，有可能多个原始数据计算出来的MD5值是一样的，这就是碰撞。
3. **不可逆**：也就是说如果告诉你一个MD5值，你是无法通过它还原出它的原始数据的，这不是你的技术不够牛，这是由它的算法所决定的。因为根据第4点，一个给定的MD5值是可能对应多个原始数据的，并且理论上讲是可以对应无限多个原始数据，所有无法确定到底是由哪个原始数据产生的。

#### sha1——示例d033e22ae348aeb5660fc2140aec35850c4da997

这种加密的密文特征跟MD5差不多，只不过位数是40。

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

## 状态响应码

### 304

HTTP 304 表示如果客户端发送了一个带条件的GET请求且该请求已被允许，而文档的内容（自上次访问以来或者根据请求的条件）并没有改变，则服务器应当返回这个状态码。304响应禁止包含消息体，因此始终以消息头后的第一个空行结尾。该响应必须包含以下头信息：Date、ETag、Content-Location、Expires、Cache-Control、Vary

## 目录

### 目录等级

* "./"：代表目前所在的目录。
* " . ./"代表上一层目录。
* "/"：代表根目录。