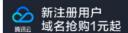
服务器常用软件 脚本之家 源市场 手机版 投稿中心 关注微信 快捷导航



1万1 1000元收 (满10元可随时结算 质量越好价格越高, 最高可达2000元





立即抢购

网页制作

网络编程

脚木专栏

脚木下裁

数据库

CMS教程

电子书籍

平面设计

媒体动画

其它

基础应用

实用技巧 白学过程

云数据库Redis版 最高10万QPS,宕机秒级拉起 (一) 阿里云







小程序普惠节 精美模板1元选购 开发套餐30元/月起



*****高防免备案CDN*****

1G香港云49元/美国云49元/韩国云89元

服务器租用/托管-域名空间/认准腾佑科技 **香港高防10m大带宽独服,低至999元**

中原地区核心数据中心,首月托管免费

免备vps20/百独799/双线350/45互联 畅游网络 百独服务器 包跑满 998元

好系统,装机首选好系统 ◆◆◆海西数据全球服务器租用◆◆◆ ★美国/香港/国内/高防服务器VPS★好优云

立即选购

★★★香港服务器租用100M促销★★★ 知了云,OpenStack云服务器+5折优惠+

云彩网络<mark>11</mark>100G防服务器450元

韩国香港美国站群服务器 巨牛网络

服务器租用 199元起

九九数据 — 工信部认可正规资质IDC接入商 浦东数据中心上海电信4星云主机30元/月起

鼎点网络百兆独享服务器仅需999元 ■5M独享云主机599/年■■■

95IDC 香港沙田CN2服务器 599/月

阿里云/腾讯云/百度云等/量大从优

4核独服199/16核独服360|创梦网络

【3000个备案老域名】100元起 每天更新

产品发布、创业开店、需求任务找大师兄

沈阳迅云

自建大连高防机房

火爆抢购

优惠一: 2核4G2м**33.9元**

30余款阿里云产品免费6个月>>

怎样购买服务器更划算?

【亿恩】DELL品牌服务器,月付799元起

★☆云服务器5折,天天抽红包抵扣☆★

港湾网络-徐州百独16核32G 999/月~

枫信科技-江苏双线10M保证-399/元

[香港双高防]无视CC★DDOS/堪比广东!

群英云服务器送10M带宽30G防御,49元起

_{优惠二:充值最高}返现500元

立即参与

西部数码 中国云主机领导品牌 仅需

云主机

(一) 阿里云 <mark>键部署</mark>云服务器环境 官方源镜像、安全稳定、免配置



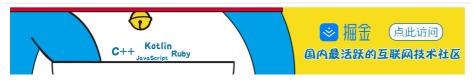
您的位置: 首页 \rightarrow 网络编程 \rightarrow ASP.NET \rightarrow 实用技巧 \rightarrow 在ASP.Net中实现RSA加密的方法

请输入关键词

在ASP.Net中实现RSA加密的方法

(转载) 2013-11-07 作者: ··· 我要评论

这篇文章介绍了在ASP.Net中实现RSA加密的方法,有需要的朋友可以参考一下



在我们实际运用中,加密是保证数据安全的重要手段。以前使用ASP时,对数据加密可以使用MD5和SHA1算法, 这两种算法虽然快捷有效,但是无法对通过它们加密的密文进行反运算,即是解密。因此需要解密数据的场合,这 两种方法就不太适合了。当然你也可以自己编写适用的加密和解密程序,不过这对编写者的数学水平有很高的要 求,一般人是很难做到的。

现在,随着ASP.Net的推出,彻底改变了以前ASP下的编程模式。我们能够利用.Net Framework中的类提供的加密 服务来保证数据安全。目前应用较为广泛的加密方法是使用RSA算法进行加密。在.Net Framework中与RSA加密算 法相关的类主要有两个: RSA 类和RSACryptoServiceProvider 类。按照MSDN的说法RSA 类是"表示 RSA 算法的所 有实现均从中继承的基类", 而RSACryptoServiceProvider 类是"使用加密服务提供程序 (CSP) 提供的 RSA 算法的 实现执行不对称加密和解密"。另外,"表示 RSA 算法的标准参数"的RSAParameters 结构也是很重要的,它保存了 RSA算法的参数。

由于介绍RSA算法原理的文章或书籍比较多,大家可以参阅一下,在此就不复述了。下面着重介绍一下如何在ASP. Net中实现RSA加密。

大家感兴趣的内容

- 1 JAVA正则表达式 Pattern和Matche
- asp.net(c#)网页跳转七种方法小结
- 未将对象引用设置到对象的实例(
- 未能加载文件或程序集 "XXX" 或它
- asp.net "服务器应用程序不可用" 5
- 6 ASP.NET中的几种弹出框提示基本实
- 7 asp.net gridview 72般绝技
- asp.net生成Excel并导出下载五种
- asp.net UpdatePanel的简单用法
- 10 ASP.NET对路径"xxxxx"

RSA参数的产生:RSA参数的类型就是上面提到的RSAParameters 结构,查阅MSDN可知其包含了D、DP、DQ、Ex ponent、InverseQ、Modulus、P、Q八个字段。加密时仅需要Exponent和Modulus两个值,可看成公钥。解密时所有字段都需要,可看成私钥。下面这段程序显示了如何产生RSA两个参数:

```
RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
RSAParameters rsaParamsExcludePrivate=rsa.ExportParameters(false);
RSAParameters rsaParamsIncludePrivate=rsa.ExportParameters(true);
```

RSACryptoServiceProvider类的ExportParameters(bool)方法用于导出RSA参数, true表示导出上述八个字段的"私钥", false表示导出"公钥"。

使用RSA参数进行加密解密:这一步需要把上面两个参数导入到RSACryptoServiceProvider类对象中,再用它对数据进行加密。如下面的代码所示,我们可以写一个函数来完成加密过程:

```
代码如下: 复制代码

Public byte [ ] RSAEncrypt ( byte [ ] b)
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.ImportParameters(rsaParamsExcludePrivate); //导入公钥
    byte [] EncryptedData=rsa.Encrypt(DataToEncrypt,false);
    return EncryptedData;
}
```

解密时只要把rsa.ImportParameters(rsaParamsExcludePrivate)换成rsa.ImportParameters(rsaParamsExcludePrivate),再把Encrypt换成Decrypt就行了。

保存和加载RSA参数:RSA参数可以保存为XML格式,下面代码说明了如何保存和加载(只列出了关键部分)

```
代码如下: 复制代码

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
StreamWriter writer=new StreamWriter(@"d:\PublicAndPrivateKey.xml");
string PPKeyXml=rsa.ToXmlString(true);//保存私钥 writer.Write(PPKeyXml);
writer.Close();
writer=new StreamWriter(@"d:\PublicKey.xml");
string PKeyXml=rsa.ToXmlString(false);//保存公钥
writer.Write(PKeyXml);
writer.Close();
```

读取:

保存:

```
代码如下: 复制代码
RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
StreamReader reader=new StreamReader(@"d:\PublicKey.xml");
string PKey=reader.ReadToEnd();
rsa.FromXmlString(PKey);
reader.Close();
StreamReader reader=new StreamReader(@"d:\PublicAndPrivateKey.xml");
string PPKey=reader.ReadToEnd();
reader.Close();
```

ToXmlString和ExportParameters方法类似,false表示保存"公钥",true表示保存"私钥"。

您可能感兴趣的文章:

ASP.net中md5加密码的方法 asp.net TripleDES加密、解密算法 asp.net下常用的加密算法MD5、SHA-1应用代码



最近更新的内容

详解ASP.NET Core 在 JSON 文件中配...
.NET 缓存设计的使用说明
asp.net窗体操作总结
.Net core下直接执行SQL语句并生成D...
asp.net 弹出警告窗口实现代码
ASP.NET 页面中加添加用户控件的写法
javascript操作ASP.NET服务器控件
[c#]asp.ent下开发中Tag的开发技巧
数据库 数据类型float到C#类型decim...
asp.net(vb)实现金额转换成大写的函数

众生网络 品牌服务器租用 集思网络

枫信科技 IDC服务商

常用在线小工具

CSS代码工具

JavaScript代码格式化工具

在线XML格式化/压缩工具

php代码在线格式化美化工具

sql代码在线格式化美化工具

在线HTML转义/反转义工具

在线JSON代码检验/检验/美化/格式化

JavaScript正则在线测试工具

在线生成二维码工具(加强版)

更多在线工具



亿息云(2核-2G-60G-3M)