

# 軟體主廚的程式料理廚房

軟體跟料理一樣，都變成了每人每天的生活必需品。

2015-12-23

## [食譜好菜] C# RSA 非對稱加密演算法

👁 9360 💬 0 📄 C# ⓘ 🔄 2016-04-30

RSA 加密演算法是一種非對稱加密演算法，網路上已經很有非常多的範例了，我只是將我的 Sample 備份在這邊，以便將來可以參考，以下節錄我有參考到的前輩們的文章。

- 余小章 @ 大內殿堂：[C#.NET] 字串及檔案，利用 RSA 演算法加解密
- 當麻許的超技八：[C#] 關於RSA 加密長度問題
- 程式勞工的汗水：[C#]RSA 加密長度錯誤

### 產生公鑰及私鑰

```
private Tuple<string, string> GenerateRSAKeys()
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

    var publicKey = rsa.ToXmlString(false);
    var privateKey = rsa.ToXmlString(true);

    return Tuple.Create<string, string>(publicKey, privateKey);
}
```

### 加密字串

```
private string Encrypt(string publicKey, string content)
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString(publicKey);

    var encryptString = Convert.ToBase64String(rsa.Encrypt(Encoding.UTF8.GetBytes(content), false));

    return encryptString;
}
```

### 解密字串

```
private string Decrypt(string privateKey, string encryptedContent)
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString(privateKey);

    var decryptString =
    Encoding.UTF8.GetString(rsa.Decrypt(Convert.FromBase64String(encryptedContent), false));
}
```

請用「空白」區分關鍵字



### 軟體廚房



Developer Technologies (2016-2021)

### SkillTree 好課程



### 技術專家的家

- Scott Hanselman
- Ruddy Lee (李智樺)
- Huan-Lin 學習筆記
- In 91
- mrkt 的程式學習筆記
- 黑暗執行緒
- .NET Walker (董大偉)
- The Will Will Web (保哥)
- gipi的學習筆記
- Ant's ATField
- Artech
- Cash Wu Geek

### 標籤雲

.NET Core Android AngularJS  
AOP App Service **ASP.NET**  
**ASP.NET Core** ASP.NET MVC  
Azure **C#** Cache-Control  
**CentOS** CI Dapper Directive

## 加密檔案

```
private void EncryptFile(string publicKey, string rawFilePath, string encryptedFilePath)
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString(publicKey);

    using (FileStream testDataStream = File.OpenRead(rawFilePath))
    using (FileStream encryptpStream = File.OpenWrite(encryptedFilePath))
    {
        var testDataByteArray = new byte[testDataStream.Length];
        testDataStream.Read(testDataByteArray, 0, testDataByteArray.Length);

        var encryptDataByteArray = rsa.Encrypt(testDataByteArray, false);

        encryptpStream.Write(encryptDataByteArray, 0, encryptDataByteArray.Length);
    }
}
```

## 解密檔案

```
private void DecryptFile(string privateKey, string encryptedFilePath, string
decryptedFilePath)
{
    RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString(privateKey);

    using (FileStream encryptpStream = File.OpenRead(encryptedFilePath))
    using (FileStream decryptpStream = File.OpenWrite(decryptedFilePath))
    {
        var encryptDataByteArray = new byte[encryptpStream.Length];
        encryptpStream.Read(encryptDataByteArray, 0, encryptDataByteArray.Length);

        var decryptDataByteArray = rsa.Decrypt(encryptDataByteArray, false);

        decryptpStream.Write(decryptDataByteArray, 0, decryptDataByteArray.Length);
    }
}
```

在加密檔案的過程當中發生了長度錯誤的例外錯誤訊息，原來加密的 KeySize 大小會影響可加密的資料內容大小，可加密的資料內容大小估算公式為  $(\text{KeySize} / 8) - 11$ 。

如果想要改變 KeySize 大小，可以在宣告 RSACryptoServiceProvider 時就指定給它，例如：  
RSACryptoServiceProvider rsa = new RSACryptoServiceProvider(2048); 就將 KeySize 大小指定為 2048。

< [Source Code](#) >

C# 指南

ASP.NET 教學

ASP.NET MVC 指引

Azure SQL Database 教學

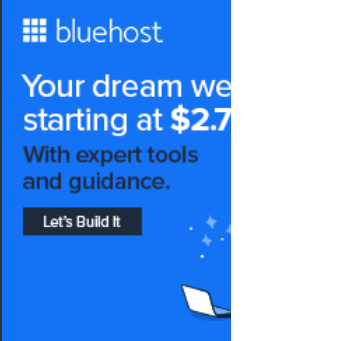
SQL Server 教學

Xamarin.Forms 教學

點部落 首頁 RSS 登入  
iOS Intermediate Language MVC  
JavaScript Jenkins jQuery  
Nginx Redis SEO Specflow  
Server StackExchange.Redis TDD  
UnitTest Windows Windows 10  
Xamarin.Forms

## 系列文章

- C# (47)
- SQL Server (19)
- CI (14)
- Jenkins (4)
- Windows Forms (4)
- Entity Framework (3)
- ELK (3)
- Selenium (2)
- CKEditor (1)
- Topshelf (1)
- Chef.DbAccess (1)
- 程式設計原則 (1)

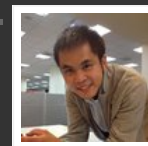


bluehost  
Your dream website  
starting at \$2.75  
With expert tools  
and guidance.  
Let's Build It

## 本頁段落

- [這裡有一個標題](#)
- [這裡有第二個標題](#)
- [又有一個標題](#)

## 最新留言



SuperShowwei

感謝 Ian 大...

[回首頁](#)

## 5 步驟教您製作高品質動畫

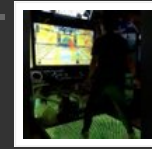
iClone 完美串接各大動畫、遊戲引擎平台，讓您為動畫電影、VR、遊戲輕鬆製作高品質專業動畫

Reallusion

### 關聯文章

- [食譜好菜] 能不能講一下什麼是泛型（Generics）？
- [小菜一碟] 將 2 的 n 次方加總結果再拆解回來
- [小菜一碟] Autofac.Extras.DynamicProxy 中 EnableInterfaceInterceptors() 及 EnableClassInterceptors() 的區別
- [料理佳餚] C# 一個 Open Source 的 Compile-time AOP 框架 - AspectInjector
- [創意料理] 生平第一次使用 >>（右移）、<<（左移）運算子就獻給 Base32 了
- [廚餘回收] 中了一個 C# 模式比對（Pattern Matching）var 的陷阱
- [料理佳餚] C# 在 Redis 發生 Failover 時自動跟著執行 HA 切換
- [小菜一碟] 檔案目前位置取得方法的不同，而不是不同的檔案目前位置取得方法。
- [料理佳餚] 用 SemaphoreSlim 來做 async/await 的鎖定
- [食譜好菜] 檔案及資料夾的路徑不用自己兜，讓 System.IO.Path 靜態類別來做會方便許多。
- [料理佳餚] 在執行時期（Runtime）憑空捏造一個型別（Type）
- [食譜小菜] 如何知道一個 Task 執行逾時？
- [料理佳餚] C# 用 Google Analytics Reporting API 來抓取特定 URL 的 PageView
- [廚餘回收] 扒網頁扒到「伺服器認可通訊協定違規. Section=...」追追追
- [料理佳餚] C# 三種實作跨應用程式鎖定的方式
- [食譜好菜] 常在面試出現的題目：SQL Injection
- [食譜好菜] 用 SqlBulkCopy 可以快速批次 Insert 大量資料，那批次 Update 大量資料呢？
- [料理佳餚] 用 ValueTuple 解放雞肋類別
- [料理佳餚] C# NEST 操作 Elasticsearch 搜尋服務（傳回部分欄位、刪除索引）
- [創意料理] 用 IL Code 來做一個簡易版本的 FastMember
- [料理佳餚] C# Microsoft.Hadoop.WebClient 執行 HDFS 基本檔案操作
- [食譜好菜] 用 Dapper 取得一對一關係、一對多關係及多型資料結構的資料都只需要一次 Query
- [料理佳餚] 將 Function 序列化為二進位資料之後傳遞給另一個應用程式執行
- [料理佳餚] C# Microsoft.Hadoop.WebClient 讀取 Hadoop Archives（HAR Files）

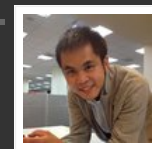
ConfigurationElement 節點內的設定值？ | 軟體主廚的程式料理廚房 - 點部落 · 1 month ago



IanChen

標題錯字？如果=>如何

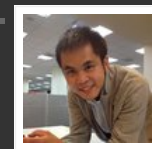
[小菜一碟] 如果讀取自訂 ConfigurationElement 節點內的設定值？ | 軟體主廚的程式料理廚房 - 點部落 · 1 month ago



SuperShowwei

感謝 Bill 叔的分享，原來這個語法在 C# 的語言規格裡面就有寫了。...

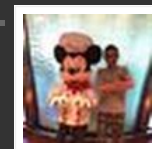
[小菜一碟] C# 初始化物件（Object Initializer）中一個冷門的語法 - 「Xyz = { ... }」 | 軟體主廚的程式料理廚房 - 點部落 · 3 months ago



SuperShowwei

推，便宜好用，是真 · 佛心軟體。

[料理佳餚] 在 Windows Server 2016/2019 建立 RAM Disk | 軟體主廚的程式料理廚房 - 點部落 · 4 months ago



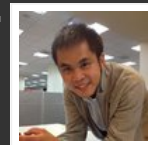
Bruce Chen

SoftPerfect RAM Disk 真的推，一套沒幾塊錢，我在某次特價還買到號稱永久更新的50年更新版。

[料理佳餚] 在 Windows Server 2016/2019 建立 RAM Disk | 軟體主

- [桌邊服務] DateTime 本身有沒有包含時區的資訊？
- [創意料理] 突發奇想的「延遲依賴注入（Lazy Dependency Injection）」
- [料理佳餚] System.IO.Pipelines 解決了以往接收 NetworkStream 算位置的困擾
- [料理佳餚] C# StackExchange.Redis 使用 Redis Message Broker 服務
- [小菜一碟] C# 中一個古老的好物 - TypeConverter
- [料理佳餚] AutoMapper 中不容忽視的 Ignore() Mapping 的順序
- [料理佳餚] C# NEST 操作 Elasticsearch 搜尋服務（搜尋、排序結果）
- [料理佳餚] C# NEST 操作 Elasticsearch 搜尋服務（建立連線、索引資料）
- [小菜一碟] 如何查看 C# 編譯出來的 IL Code？
- [創意料理] 用 Expression 做一個簡易的 Object-Object Mapping
- [料理佳餚] Dapper 用起來很友善，但是預設的參數型別對執行計劃不太友善。
- [食譜好菜] 用 SqlBulkCopy 批次 Insert 大量資料讓你意想不到的快
- [料理佳餚] 讓 FluentValidation 把參數的檢查條件口語化
- [小菜一碟] Trim() 不只能修剪空白字元而已
- [料理佳餚] 使用 Decorator Pattern 分離參數檢查與資料處理
- [小菜一碟] 發現一個小玩意兒 - TaskCompletionSource
- [小菜一碟] C# 的 double 在 SQL Server 應該要存成 float，搞清楚單精度跟雙精度的差別。
- [食譜好菜] DateTime 具有文化特性的格式化及時區的轉換
- [食譜好菜] Json.NET 處理多型的反序列化
- [料理佳餚] C# 使用 Google APIs 來控制 GCE（Google Compute Engine）VM 的開啟跟關閉
- [料理佳餚] C# 泛型類別條件約束 where 無法約束帶有參數的建構式怎麼辦？
- [料理佳餚] C# ServiceStack.Redis 使用 Redis 的 Cache 及 Message Broker 服務
- [廚餘回收] 扒網頁扒到「伺服器認可通訊協定違規. Section=...」（伺服器認可的耶）
- [料理佳餚] C# StackExchange.Redis 存取 Redis Cache 服務
- [食譜好菜] 用 SonarQube 分析 C# 程式碼品質
- [食譜好菜] 從 C# 一個簡單的 lock string 修正了對 String Pool 的觀念
- [廚餘回收] Windows 工作排程器（Task Scheduler）啟動程式取得與執行檔所在相同目錄
- [小菜一碟] C# 中的奇門遁甲 - 隱含轉換（implicit）
- [料理佳餚] FluentValidation + Autofac.Extras.DynamicProxy2 實現參數條件檢查的 AOP 攔截器
- [料理佳餚] 使用 log4net
- [料理佳餚] 用 C# 的 System.Reflection.Emit 撰寫 IL Code 將值指派給私有欄位（Private Field）
- [小菜一碟] 如何讀取自訂 ConfigurationElement 節點內的設定值？
- [料理佳餚] 自製 NLog 的 Target（以 Slack 的 Incoming WebHooks 為例）
- [料理佳餚] C# 實作二階段提交（Two-phase Commit），即使 SQL Server 沒有啟用 MSDTC 也能做分散式交易。
- [小菜一碟] 取得往上第 n 個階層的目錄路徑

months ago



SuperShowwei

謝謝現金大大的分享，小弟受用無窮。

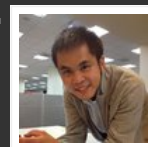
[料理佳餚] C# 一個 Open Source 的 Compile-time AOP 框架 - AspectInjector | 軟體主廚的程式料理廚房 - 點部落 · 7 months ago



Cash

感謝大大分享，參考你的文章和官方的代碼寫了一個可以用在 autofac 的 Cache XD...

[料理佳餚] C# 一個 Open Source 的 Compile-time AOP 框架 - AspectInjector | 軟體主廚的程式料理廚房 - 點部落 · 7 months ago



SuperShowwei

指定 Listen 的 IP 可以像下圖這樣做...

[料理佳餚] 除了 Web API 之外的新選擇 - gRPC 服務 | 軟體主廚的程式料理廚房 - 點部落 · 9 months ago

[食譜好菜] C# DES 對稱加密演算法使用不固定長度的 Key 及 IV 進行加解密

## 系列文章

[料理佳餚] 使用 log4net

[食譜好菜] C# RSA 非對稱加密演算法

[料理佳餚] C# 切換 Windows Form 的執行身分

[食譜好菜] 常在面試出現的題目：SQL Injection

[食譜好菜] 能不能講一下什麼是泛型（Generics）？

[料理佳餚] 讓 FluentValidation 把參數的檢查條件口語化

[料理佳餚] FluentValidation + Autofac.Extras.DynamicProxy2 實現參數條件檢查的 AOP 攔截器

[廚餘回收] 扒網頁扒到「伺服器認可通訊協定違規. Section=...」（伺服器認可的耶）

[廚餘回收] 扒網頁扒到「伺服器認可通訊協定違規. Section=...」追追追

[食譜好菜] DateTime 具有文化特性的格式化及時區的轉換

[食譜好菜] 用 SqlBulkCopy 批次 Insert 大量資料讓你意想不到的快

[小菜一碟] 取得往上第 n 個階層的目錄路徑

[料理佳餚] C# 在 Redis 發生 Failover 時自動跟著執行 HA 切換

[食譜好菜] 從 C# 一個簡單的 lock string 修正了對 String Pool 的觀念

[小菜一碟] Autofac.Extras.DynamicProxy 中 EnableInterfaceInterceptors() 及 EnableClassInterceptors() 的區別

[食譜好菜] 用 Dapper 取得一對一關係、一對多關係及多型資料結構的資料都只需要一次 Query

[料理佳餚] 將 Function 序列化為二進位資料之後傳遞給另一個應用程式執行

[食譜小菜] 如何知道一個 Task 執行逾時？

[小菜一碟] 發現一個小玩意兒 - TaskCompletionSource

[廚餘回收] Windows 工作排程器（Task Scheduler）啟動程式取得與執行檔所在相同目錄

[食譜好菜] 檔案及資料夾的路徑不用自己兜，讓 System.IO.Path 靜態類別來做會方便許多。

[料理佳餚] 用 ValueTuple 解放雞肋類別

[食譜好菜] Json.NET 處理多型的反序列化

[創意料理] 生平第一次使用 >>（右移）、<<（左移）運算子就獻給 Base32 了

[小菜一碟] 檔案目前位置取得方法的不同，而不是不同的檔案目前位置取得方法。

[料理佳餚] C# 三種實作跨應用程式鎖定的方式

[料理佳餚] C# 實作二階段提交（Two-phase Commit），即使 SQL Server 沒有啟用 MSDTC 也能做分散式交易。

[小菜一碟] 將 2 的 n 次方加總結果再拆解回來

[料理佳餚] C# 用 Google Analytics Reporting API 來抓取特定 URL 的 PageView

[桌邊服務] DateTime 本身有沒有包含時區的資訊？

[小菜一碟] C# 中一個古老的好物 - TypeConverter

- [料理佳餚] System.IO.Pipelines 解決了以往接收 NetworkStream 算位置的困擾
- [料理佳餚] C# 泛型類別條件約束 where 無法約束帶有參數的建構式怎麼辦？
- [料理佳餚] Dapper 用起來很友善，但是預設的參數型別對執行計劃不太友善。
- [小菜一碟] Trim() 不只能修剪空白字元而已
- [廚餘回收] 中了一個 C# 模式比對（Pattern Matching）var 的陷阱
- [小菜一碟] C# 的 double 在 SQL Server 應該要存成 float，搞清楚單精度跟雙精度的差別。
- [料理佳餚] 用 SemaphoreSlim 來做 async/await 的鎖定
- [創意料理] 用 Expression 做一個簡易的 Object-Object Mapping
- [料理佳餚] 自製 NLog 的 Target（以 Slack 的 Incoming WebHooks 為例）
- [料理佳餚] C# 一個 Open Source 的 Compile-time AOP 框架 - AspectInjector
- [小菜一碟] C# 初始化物件（Object Initializer）中一個鮮少用到的冷門語法 - 「Xyz = { ... }」
- [料理佳餚] 用 C# 的 System.Reflection.Emit 撰寫 IL Code 將值指派給私有欄位（Private Field）
- [小菜一碟] 如何查看 C# 編譯出來的 IL Code？
- [料理佳餚] 在執行時期（Runtime）憑空捏造一個型別（Type）
- [創意料理] 用 IL Code 來做一個簡易版本的 FastMember

ALSO ON 軟體主廚的程式料理廚房

**[料理佳餚] C# 泛型類別條件約束 where ...**

2年前 • 2 comments

公司內的一個系統的開發風格轉變，Data Model 必須設計成 ...

**[料理佳餚] 用 SemaphoreSlim 來做 ...**

一年前 • 2 comments

在 C# 應用程式內部要做鎖定，第一時間我們一定是先想到 lock 陳述式，但是 ...

**[料理佳餚] ASP.NET Core 撰寫 ...**

一年前 • 2 comments

在前一篇文章 [料理佳餚] ASP.NET Core 的虛擬目錄哪去了？中有提到，傳統 ...

**[桌邊服務] 將 MVC 的 View ...**

2年前 • 5 comments

各位朋友應該都需求，就是有一個頁面服務的是 ...

0 Comments

軟體主廚的程式料理廚房

Disqus' Privacy Policy

1 Login

Recommend

Tweet

Share

Sort by Best

Start the discussion...