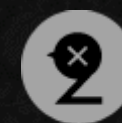


當麻許的超技八

超自然、技術、八卦 - 兼任的偽善者，職業的詐欺師，part-time的故事家，業餘的code generator，不服輸的夢想家，長不大的幼稚鬼，Facebook超自然現象研究社社長，堅持對我來說 就是以剛克剛。



Home



RSS



github

[C#] 與Android共舞-AES 加解密(Android 端)

2013年3月13日

上一篇文章 [\[C#\] 與Android共舞-AES 加密\(C# 端\)](#) 我們提到 我們在 C# 端使用AES 256 進行加密，其Key IV 如下：

```
// 32 個英文或數字
string key = "1234567890" +
             "1234567890" +
             "1234567890" +
             "12";

// 16 個英文或數字
string iv = "1234567890" +
            "abcdef";
```

現在，我們來看看Android 端的地方如何解密
Andoird Code 解密端：

```
public static byte[] decryptAES (byte[] ivBytes, byte[] keyBytes,byte[] textBytes) {
    try {
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes);

        SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

        cipher.init(Cipher.DECRYPT_MODE, newKey, ivSpec);
```

廣告區

Visual Studio Community

無料下載



Windows 10

取得SDK



設計 UWP

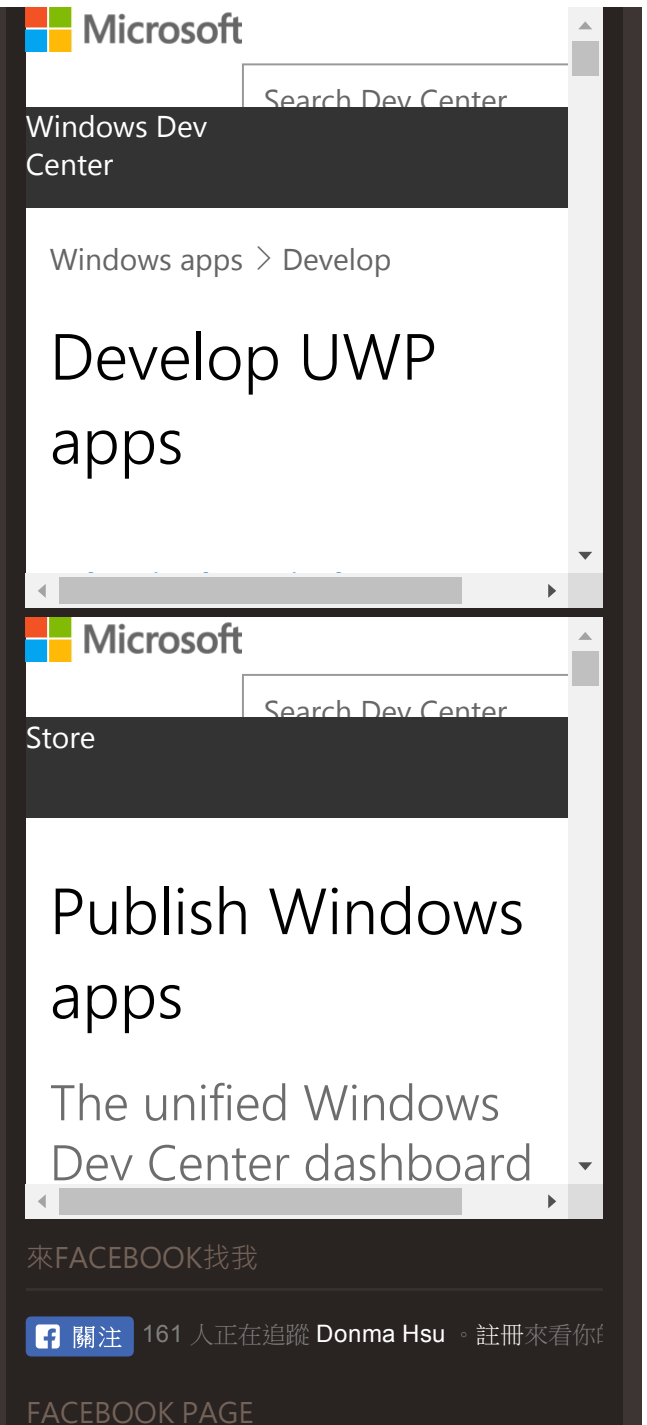
從零開始

```
        return cipher.doFinal(textBytes);  
    } catch (Exception ex) {  
        return null;  
    }  
}
```

呼叫 解密:

```
try{  
  
String key="12345678901234567890123456789012";  
String iv="1234567890abcdef";  
String encryptString="wifhXJU46ETengY/nA+sGQ==";  
  
byte[] descryptBytes=decryptAES(iv.getBytes("UTF-8"),key.getBytes("UTF-8"),Base64.decode(encryptString));  
  
Toast.makeText(this,new String(descryptBytes), Toast.LENGTH_LONG).show();  
  
}catch(Exception ex){}
```

結果:





OK 解密完成 · 順便附上 加密的 function

```
public static byte[] encryptAES(byte[] ivBytes, byte[] keyBytes, byte[] textBytes) {  
  
    try {  
  
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes);
```



微博

```

    SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");

    Cipher cipher = null;

    cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

    cipher.init(Cipher.ENCRYPT_MODE, newKey, ivSpec);

    return cipher.doFinal(textBytes);

} catch (Exception ex) {

    return null;

}

}

```


文章參考來源


<https://gist.github.com/dealforest/1949873>

標籤： [Android](#) [C#](#)

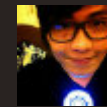
--

請你暫時把你的勇氣給我 在夢想快消失的時候 讓我的 Code 用力的穿過天空 為愛我的人做一秒英雄 如果這篇文章有幫助到您，簡單留個言，或是幫我按個讚，讓我有寫下去的動力...

 讚好 [分享](#) 11 人對此讚好。趕快註冊來看看朋友對哪些內容讚好。

 在 Google 上推薦這個網址

 微博



當麻許 台灣 台北

[+ 加关注](#)

我覺得我的了一種買不起手機瘋狂看大家發布會跟測評的病，還是我找一個手機測評機構去應徵好了...

2016-10-27 11:49

[转发](#) | [评论](#)

其實我很喜歡槌子他追求細節無與倫比，但是小米Note2 出來在這強大的規格下.. 一樣的錢我可能還是會買小米Note2 ..

2016-10-27 11:48

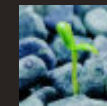
[转发](#) | [评论](#)

TA 的粉丝 (312)

[全部»](#)



1YDS芳



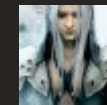
米亚刷脂



3045249



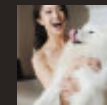
生日报19



怒奔



清华土匪



可爱多飞



疲憊的白

站內搜尋

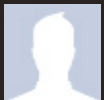
[衝](#)

標籤們

[.Net\(29\)](#)

0則回應

排序方式: 最舊 ▼



新增回應.....

Facebook Comments Plugin

[較新的文章](#)[首頁](#)[較舊的文章](#)

- ▶▶ [程式心理學](#) (2)
- ▶▶ [超自然現象研究社](#) (4)
- ▶▶ [開箱](#) (6)
- ▶▶ [業配](#) (1)
- ▶▶ [電影](#) (1)
- ▶▶ [說好今夜不談程式](#) (23)
- ▶▶ [隨貼即用](#) (27)
- ▶▶ [濾鏡](#) (12)
- ▶▶ [ActionScript](#) (1)
- ▶▶ [Android](#) (83)
- ▶▶ [Arduino](#) (1)
- ▶▶ [ASP.net](#) (85)
- ▶▶ [Azure](#) (3)
- ▶▶ [C](#) (7)
- ▶▶ [C#](#) (269)
- ▶▶ [Cordova](#) (1)
- ▶▶ [Cracker](#) (1)
- ▶▶ [Eclipse](#) (1)
- ▶▶ [ErrorLog](#) (2)
- ▶▶ [Facebook](#) (8)
- ▶▶ [Flex](#) (1)
- ▶▶ [GOOGLE](#) (5)
- ▶▶ [HACK](#) (1)
- ▶▶ [IE9](#) (1)
- ▶▶ [Internet Explorer](#) (1)
- ▶▶ [IoT](#) (6)
- ▶▶ [Javascript](#) (38)
- ▶▶ [JSON](#) (11)

- » [Lia](#) (3)
- » [Linkit7688](#) (3)
- » [Linux](#) (4)
- » [Lucene.net](#) (22)
- » [MANTIS](#) (2)
- » [MySQL](#) (2)
- » [NDK](#) (4)
- » [Node.js](#) (9)
- » [NoSQL](#) (8)
- » [office](#) (6)
- » [Omnia 7](#) (2)
- » [OpenSource](#) (4)
- » [OrangePi](#) (1)
- » [PhoneGap](#) (3)
- » [PHP](#) (2)
- » [Raspberry Pi](#) (1)
- » [Regex](#) (5)
- » [RPi](#) (1)
- » [RTSP](#) (1)
- » [SEO](#) (2)
- » [Silverlight](#) (17)
- » [SoX](#) (1)
- » [TFS](#) (1)
- » [Trick](#) (25)
- » [UMA](#) (1)
- » [UWP](#) (5)
- » [Visual Studio](#) (7)
- » [Visual Studio Code](#) (1)

- » [WebService](#) (7)
- » [WebTest](#) (1)
- » [WIN10](#) (7)
- » [Windows8](#) (11)
- » [WindowsPhone](#) (44)
- » [Winform](#) (9)
- » [Winform](#) (1)
- » [Xamarin](#) (73)
- » [XAML](#) (2)
- » [XML](#) (4)

連結們

- » [Github](#)
- » [Xamarin Components](#)
- » [超自然現象研究社@Facebook](#)
- » [當麻許@點部落](#)
- » [Windows Dev @ Channel 9](#)
- » [發佈 Windows app](#)
- » [開發 Windows app](#)

網誌存檔

- 2017 (22)
- 2016 (45)
- 2015 (46)
- 2014 (12)
- ▼ 2013 (102)
 - 十一月 (3)
 - 十月 (21)

▶ 九月 (7)

▶ 八月 (12)

▶ 七月 (20)

▶ 六月 (12)

▶ 五月 (4)

▶ 四月 (2)

▼ 三月 (6)

[\[C#\] 第一次自己作 Captcha\(驗證碼\) 就上手 \(3\)](#)

[\[C#\] 與Android共舞-AES 加解密\(Android 端\)](#)

[\[C#\] 與Android共舞-AES 加解密\(C# 端\)](#)

[\[C#\] 第一次自己作 Captcha\(驗證碼\) 就上手 \(2\)](#)

[\[C#\] 第一次自己作 Captcha\(驗證碼\) 就上手 \(1\)](#)

[\[Android\] 懶人改變Eclipse的Coding style.](#)

▶ 二月 (11)

▶ 一月 (4)

▶ 2012 (137)

AUTHOR

[+當麻許](#)

[在 Google+ 追蹤當麻](#)

當麻許的超技八 2014 | Design: no2don.