

阿里云实时计算训练营重磅升级

结营抢 天猫精灵 & 独家实物好礼

点我免费报名

博客園

cnblogs.com

首頁

新聞

博問

專區

閃存

班級

代碼改變世界

註冊

登錄

大樹下玩耍

OpenSSL.Net使用隨記（四）

ECDSA簽名算法

• ECDSA

```
1 class Program_ECDSA
2 {
3     static void Main( string [] args)
4     {
5         byte [] messageBytes = Encoding.UTF8.GetBytes( " ECDSA" );
6
7         byte [] signBytes = Sign(privateKey, messageBytes);
8         bool result = Verify(publicKey, messageBytes, signBytes);
9         Console.WriteLine(result);
10
11         signBytes = Sign512(privateKey, messageBytes);
12         result =Verify512(publicKey, messageBytes, signBytes);
13         Console.WriteLine(result);
14         Console.ReadKey();
15     }
16
17     static string privateKey = @"-----BEGIN EC PARAMETERS-----
18 BgUrgQQAIw=
19 -----END EC PARAMETERS-----
20 -----BEGIN EC PRIVATE KEY-----
21 MIHcAgEBBEIAzb3CKEl2y87QldbqiOCG0UkBceI9V5nA4N0vXZx7xgJTHtfHCe!
22 y/72GTzk7PQw89aTU7fdQl2NRC2hYiP2O1WgBwYFK4EEACOhgYkDgYYABAEwtG"
23 5cGCineqYs3VPHdad0JgIwd0BGkuSEOWt3RD1lS50iBpY0bVYkYHKvysZYPfvF!
24 EZOTNyNue3JZ0ubWzQDWHUL1/P9t8LZrPrIMC43sHuoHDV0BhcsO/HUWKU9QBCY!
25 S++px6BwYrNoFaenJoHOvtDs8veqH1aAAQW1Mbb56A==
26 -----END EC PRIVATE KEY-----
27 " ;
28
29     static string publicKey = @"-----BEGIN PUBLIC KEY-----
30 MIGbMABGByqGSM49AgEGBSuBBAAjA4GGAAQBMLRu0+XBgop3qmLN1Tx3WnTiYCl
31 9ARpLkhDlrd0Q9dUuTogaWNG1WJGBYr8kmWD37xSFhGtKzcbntYdLmls0Alh!
32 5fz/bfC2az6yDAuN7B7qBw1dAYXLdVx1FilPUAQmIUvvqcegcGKzaBWnpyaBz1l
33 7PL3qh9WgAEftTG2+eg=
34 -----END PUBLIC KEY-----
35 " ;
36
37     public static byte [] Sign( string privateKey, byte []
38     {
39         using (CryptoKey cryptoKey = CryptoKey.FromPrivateKe
40         {
41             using (MessageDigestContext hashDigest = new Me
```

導航

- 博客園
- 首頁
- 新隨筆
- 聯繫
- 訂閱
- 管理

公告

暱稱: Azeri  
園齡: 10年3個月  
粉絲: 4  
關注: 130  
[+加關注](#)

2021年3月						
日	一	二	三	四	五	六
28	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

統計

隨筆- 5  
文章- 0  
評論- 0  
閱讀- 6016

搜索

找找看

谷歌搜索

常用鏈接

- 我的隨筆
- 我的評論
- 我的參與
- 最新評論
- 我的標籤

我的標籤

OpenSSL.Net (4)  
SFTP (1)

隨筆檔案

2018年9月(1)  
2018年5月(2)  
2018年4月(2)

閱讀排行榜

https://www.cnblogs.com/azeri/p/8987294.html

1/3

```
42         {
43             byte [] hashBytes = hashDigest.Digest(messageBytes);
44             return hashDigest.Sign(messageBytes, cryptoKey);
45         }
46     }
47 }
48
49 public static bool Verify( string publicKey, byte [] messageBytes, byte [] signatureBytes)
50 {
51     using (CryptoKey cryptoKey = CryptoKey.FromPublicKey(publicKey))
52     {
53         using (MessageDigestContext hashDigest = new MessageDigestContext(cryptoKey))
54         {
55             byte [] hashBytes = hashDigest.Digest(messageBytes);
56             return hashDigest.Verify(messageBytes, signatureBytes, cryptoKey);
57         }
58     }
59 }
60
61 public static byte [] Sign512( string privateKey, byte [] messageBytes)
62 {
63     using (CryptoKey cryptoKey = CryptoKey.FromPrivateKey(privateKey))
64     {
65         using (MessageDigestContext hashDigest = new MessageDigestContext(cryptoKey))
66         {
67             byte [] hashBytes = hashDigest.Digest(messageBytes);
68             return hashDigest.Sign(messageBytes, cryptoKey);
69         }
70     }
71 }
72
73 public static bool Verify512( string publicKey, byte [] messageBytes, byte [] signatureBytes)
74 {
75     using (CryptoKey cryptoKey = CryptoKey.FromPublicKey(publicKey))
76     {
77         using (MessageDigestContext hashDigest = new MessageDigestContext(cryptoKey))
78         {
79             byte [] hashBytes = hashDigest.Digest(messageBytes);
80             return hashDigest.Verify(messageBytes, signatureBytes, cryptoKey);
81         }
82     }
83 }
84
85 }
```

1. SFTP免密碼登錄踏坑經歷(4521)
2. OpenSSL.Net使用隨記(536)
3. OpenSSL.Net使用隨記 (二) (331)
4. OpenSSL.Net使用隨記 (四) (321)
5. OpenSSL.Net使用隨記 (三) (304)

Powered by:

博客園

Copyright © 2021 Azeri

Powered by .NET 5.0 on Kubernetes

標籤: OpenSSL.Net

好文要頂

關注我

收藏該文



Azeri

關注- 130

粉絲- 4

+加關注

0

推荐

0

反对

« 上一篇: [OpenSSL.Net使用隨記 \(三\)](#)

» 下一篇: [SFTP免密碼登錄踏坑經歷](#)

posted on 2018-05-03 20:23 [Azeri](#) 阅读(321) 评论(0) [编辑](#) [收藏](#)

[刷新评论](#) [刷新页面](#) [返回顶部](#)

 登录后才能发表评论, 立即 [登录](#) 或 [注册](#), [访问](#) [网站首页](#)

【推荐】阿里云实时计算训练营重磅开启, 4天技能突破, 抢天猫精灵!

【推荐】阿里云春招即将开始, 提前下载面试宝典稳拿Offer

【推荐】阿里云Java训练营--就5天, 名师带你实战Spring Boot 2.5

【推荐】免费领最高6000元好云礼! 15种权益祝你云气爆棚

【推荐】大型组态、工控、仿真、CAD\GIS 50万行VC++源码免费下载!

【推荐】注册 Amazon Web Services(AWS) 账号, 成为博客园赞助者

【推荐】华为HMS Core Discovery直播间-七个推送技巧带你玩转App运营



**AWS免费产品:**

- [如何在AWS上免费构建网站](#)
- [AWS免费云存储解决方案](#)
- [在AWS上免费构建数据库](#)
- [AWS上的免费机器学习](#)



**最新新聞:**

- 國際知名AI學者陶大程出任京東探索研究院院長
  - 29歲網紅吃播“泡泡龍”去世曾靠“給自助餐廳上課”成名
  - 換電風波“劇終”！特斯拉工商變更：刪除“換電設施銷售”
  - 螞蟻森林價值首度公佈：5億人在手機上種樹種出113億
  - 影視劇中的“滴血認親”有科學依據嗎？終於明白了
- » [更多新聞...](#)