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( " ECI
6
7             byte [] signBytes = Sign(privateKey, messageBytes);
8              bool result = Verify(publicKey, messageBytes, signBy
9              Console.WriteLine(result);
10
11             signBytes = Sign512(privateKey, messageBytes);
12              result =Verify512(publicKey, messageBytes, signByte
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  MIHcAgEBBEIAzb3CKEl2y87Q1dbqiOCG0UkBceI9V5nA4N0vXZx7xgJTHtfHCe
22  y/72GTZk7PQw89aTU7fdQl2NRC2hYiP2O1WgBwYFK4EEACOhgYkDgYYABAEwtG
23  5cGCineqYs3VPHdadOJgIwD0BGkuSEOWt3RD11S5OiBpY0bVYkYHKvySZYPfvF
24 EZOTNyNue3JZ0ubWzQDWHULl/P9t8LZrPrIMC43sHuoHDV0BhcsO/HUWKU9QBCY
25  S++px6BwYrNoFaenJoHOVtDs8veqH1aAAQW1Mbb56A==
26  -----END EC PRIVATE KEY-----
27  " ;
28
29         static  string publicKey = @" -----BEGIN PUBLIC KEY----
30  MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBMLRu0+XBgop3qmLN1Tx3WnTiYC
31  9ARpLkhDlrd0Q9dUuTogaWNG1WJGByr8kmWD37xSFhGTkzcjbntyWdLm1s0A1h
32  5fz/bfC2az6yDAuN7B7qBw1dAYXLDvx1FilPUAQmIUvvqcegcGKzaBWnpyaBzl
33  7PL3qh9WgAEFtTG2+eg=
34  -----END PUBLIC KEY-----
35  " ;
36
37        public  static  byte [] Sign( string privateKey, byte []
38          {
39              using (CryptoKey cryptoKey = CryptoKey.FromPrivateK
40              {
41                  using (MessageDigestContext hashDigest = new Me
```


導航

博客園
首頁
新隨筆
聯繫
訂閱 XML
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

```
                {
                    byte [] hashBytes = hashDigest.Digest(messa
                    return hashDigest.Sign(messageBytes, crypto
                }
            }
        }

        public  static  bool Verify( string publicKey, byte [] m
        {
            using (CryptoKey cryptoKey = CryptoKey.FromPublicKe
            {
                using (MessageDigestContext hashDigest = new Me
                {
                    byte [] hashBytes = hashDigest.Digest(messa
                   return hashDigest.Verify(messageBytes, signB
                }
            }
        }

        public  static  byte [] Sign512( string privateKey, byte
        {
            using (CryptoKey cryptoKey = CryptoKey.FromPrivateK
            {
                using (MessageDigestContext hashDigest = new Me
                {
                   byte [] hashBytes = hashDigest.Digest(messag
                    return hashDigest.Sign(messageBytes, crypto
                }
            }
        }

        public  static  bool Verify512( string publicKey, byte
        {
            using (CryptoKey cryptoKey = CryptoKey.FromPublicKe
            {
                using (MessageDigestContext hashDigest =new Mes
                {
                    byte [] hashBytes = hashDigest.Digest(messa
                    return hashDigest.Verify(messageBytes, sign
                }
            }
        }

    }
```

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