- 订阅

{流火枫林}

善战者无赫赫之功
故善者之战，无奇胜，无智名，无勇功

- Google...

iOS下的RSA加密方法

作者: zsxwing 更新: 2012-03-17 15:02:10 发布: 2012-03-17 15:02:10

最近几天折腾了一下如何在iOS上使用RSA来加密。iOS上并没有直接的RSA加密API。但是iOS提供了x509的API，而x509是支持RSA加密的。因此，我们可以通过制作自签名的x509证书（由于对安全性要求不高，我们并不需要使用CA认证的证书），再调用x509的相关API来进行加密。接下来记录一下整个流程。

第一步，制作自签名的证书

1.最简单快捷的方法，打开Terminal，使用openssl（Mac OS X自带）生成私钥和自签名的x509证书。

```
openssl req -x509 -out public_key.der -outform der -new -newkey rsa:1024 -keyout private_key.pem -days 3650
```

按照命令行的提示输入内容就行了。

几个说明:

public_key.der是输出的自签名的x509证书，即我们要用的。

private_key.pem是输出的私钥，用来解密的，请妥善保管。

rsa:1024这里的1024是密钥长度，1024是比较安全的，如果需要更安全的话，可以用2048，但是加解密代价也会增加。

-days：证书过期时间，一定要加上这个参数，默认的证书过期时间是30天，一般我们不希望证书这么短就过期，所以写上比较合适的天数，例如这里的3650(10年)。

事实上，这一行命令包含了好几个步骤（我研究下面这些步骤的原因是我手头已经由一个private_key.pem私钥了，想直接用这个来生成x509证书，也就是用到了下面的2-3）

1)创建私钥

```
openssl genrsa -out private_key.pem 1024
```

2)创建证书请求（按照提示输入信息）

```
openssl req -new -out cert.csr -key private_key.pem
```

3)自签署根证书

```
openssl x509 -req -in cert.csr -out public_key.der -outform der -signkey private_key.pem -days 3650
```

2.验证证书。把public_key.der拖到xcode中，如果文件没有问题的话，那么就可以直接在xcode中打开，看到证书的各种信息。如下图所示：

lamzsx

签发者名称
国家/地区 CN
省/市/自治区 Beijing
所在地 Beijing
组织 lamzsx
组织单位 lamzsx
常用名称 lamzsx
电子邮件地址 test@iamzsx.com

序列号 00 90 F5 63 2F E5 7B 0A E1
版本 1
签名算法 带 RSA 加密的 SHA-1 (1.2.840.113549.1.1.5)
参数 无

第二步，使用public_key.der来进行加密。

1.导入Security.framework。

2.把public_key.der放到mainBundle中（一般直接拖到Xcode就行啦）。

3.从public_key.der读取公钥。

4.加密。

下面是参考代码（只能用于加密长度小于等于116字节的内容，适合于对密码进行加密。使用了ARC，不过还是要注意部分资源需要使用CFRealse来释放）

RSA.h

```
01 //
02 //  RSA.h
03 //
04 #import <Foundation/Foundation.h>
05
06 @interface RSA : NSObject {
07     SecKeyRef publicKey;
08     SecCertificateRef certificate;
09     SecPolicyRef policy;
10     SecTrustRef trust;
11     size_t maxPlainLen;
12 }
13
```

```
14 - (NSData *) encryptWithData:(NSData *)content;
15 - (NSData *) encryptWithString:(NSString *)content;
16
17 @end
```

RSA.m

```
01 //
02 //  RSA.m
03 //
04 #import "RSA.h"
05
06 @implementation RSA
07
08 - (id)init {
09     self = [super init];
10
11     NSString *publicKeyPath = [[NSBundle mainBundle]
   pathForResource:@"public_key"
12                                                     ofType:@"der"];
13     if (publicKeyPath == nil) {
14         NSLog(@"Can not find pub.der");
15         return nil;
16     }
17
18     NSDate *publicKeyFileContent = [NSData
   dataWithContentsOfFile:publicKeyPath];
19     if (publicKeyFileContent == nil) {
20         NSLog(@"Can not read from pub.der");
21         return nil;
22     }
23
24     certificate = SecCertificateCreateWithData(kCFAllocatorDefault, (
   __bridge CFDataRef)publicKeyFileContent);
25     if (certificate == nil) {
26         NSLog(@"Can not read certificate from pub.der");
27         return nil;
28     }
29
30     policy = SecPolicyCreateBasicX509();
31     OSStatus returnCode = SecTrustCreateWithCertificates(certificate,
   policy, &trust);
32     if (returnCode != 0) {
33         NSLog(@"SecTrustCreateWithCertificates fail. Error Code:
   %ld", returnCode);
34         return nil;
35     }
36
37     SecTrustResultType trustResultType;
38     returnCode = SecTrustEvaluate(trust, &trustResultType);
39     if (returnCode != 0) {
40         NSLog(@"SecTrustEvaluate fail. Error Code: %ld", returnCode);
41         return nil;
42     }
43
44     publicKey = SecTrustCopyPublicKey(trust);
45     if (publicKey == nil) {
```

```
46          NSLog(@"SecTrustCopyPublicKey fail");
47          return nil;
48      }
49
50      maxPlainLen = SecKeyGetBlockSize(publicKey) - 12;
51      return self;
52  }
53
54  - (NSData *) encryptWithData:(NSData *)content {
55
56      size_t plainLen = [content length];
57      if (plainLen > maxPlainLen) {
58          NSLog(@"content(%ld) is too long, must < %ld", plainLen,
    maxPlainLen);
59          return nil;
60      }
61
62      void *plain = malloc(plainLen);
63      [content getBytes:plain
64                 length:plainLen];
65
66      size_t cipherLen = 128; // 当前RSA的密钥长度是128字节
67      void *cipher = malloc(cipherLen);
68
69      OSStatus returnCode = SecKeyEncrypt(publicKey, kSecPaddingPKCS1,
    plain,
70                                          plainLen, cipher,
    &cipherLen);
71
72      NSData *result = nil;
73      if (returnCode != 0) {
74          NSLog(@"SecKeyEncrypt fail. Error Code: %ld", returnCode);
75      }
76      else {
77          result = [NSData dataWithBytes:cipher
78                                  length:cipherLen];
79      }
80
81      free(plain);
82      free(cipher);
83
84      return result;
85  }
86
87  - (NSData *) encryptWithString:(NSString *)content {
88      return [self encryptWithData:[content
    dataUsingEncoding:NSUTF8StringEncoding]];
89  }
90
91  - (void)dealloc{
92      CFRelease(certificate);
93      CFRelease(trust);
94      CFRelease(policy);
95      CFRelease(publicKey);
96  }
97
98  @end
```

使用方法:

```
RSA *rsa = [[RSA alloc] init];
if (rsa != nil) {
    NSLog(@"%@",[rsa encryptWithString:@"test"]);
}
else {
    NSLog(@"init rsa error");
}
```

参考:

1. （原创）如何生成以及导入X.509证书

http://hi.baidu.com/five00/blog/item/43bf1fd77df2d8d9a044df39.html

2. ios下使用rsa算法与php进行加解密通讯

http://blog.yorkgu.me/2011/10/27/rsa-in-ios-using-publick-key-generated-by-openssl/

3. Certificate, Key, and Trust Services Reference

http://developer.apple.com/library/mac/#documentation/security/Reference/certifkeytrustservices/Reference/reference.html

4. X509

http://baike.baidu.com/view/2841580.htm

5. RSA

http://zh.wikipedia.org/zh/RSA%E5%8A%A0%E5%AF%86%E6%BC%94%E7%AE%97%E6%B3%95

类别: iOS

回复

- *小罗* 说:
  2012-04-10 17:40:18
  请问，有没有ios的解密的呢？ 是否能发表……
- ***182.151.*.**** 说:
  2012-07-16 19:56:35
  请问文中说的只能对小于116字节的内容加密，是指参考代码还是？谢谢……
- ***zsxwing*** 说:
  2012-08-30 16:13:39
  加密的大小受限于SecKeyEncrypt函数，SecKeyEncrypt要求明文和密钥的长度一致，如果要加密更长的内容，需要把内容按密钥长度分成多份，然后多次调用SecKeyEncrypt来实现。
- ***124.74.*.**** 说:
  2012-10-12 17:51:31
  请问解密、签名和验签有相关demo吗？能不能支持cer加密，p12解密？
- *匿名**Nitesh*** 说:

2013-04-05 20:53:56
How to decrypt encrypted data? What will be method for decryption.?

- ***匿名Nitesh*** 说:
  2013-04-05 21:21:50
  How to get return text as "test" ? I am taking about decryption ??
- ***222.35.*.**** 说:
  2013-07-09 11:59:39
  您好 服务器只给了我一个NSString 让我来当公钥用 并没有给我证书 请问我要如何操作呢?
- ***zsxwing*** 说:
  2013-07-09 16:43:20
  你试试看这篇文章，我没有试过，不能保证OK：http://stackoverflow.com/questions/1536894/converting-raw-rsa-key-value-to-seckeyref-object-for-encryption
- ***hyc4117*** 说:
  2013-09-03 11:38:13
  求解密方法啊 大哥 谢谢啦
- ***jackyccaa*** 说:
  2014-03-26 20:53:00
  两个问题： 1. 支持cer格式的读写吗？ 2. 支持1024bit的public key的cer格式的读写不?

发表回复

匿名 昵称

提交

- # 文章类别

最新的回复

- **58.213.*.***说赞
- **zsxwing**说多谢指出错误。已改过
- **182.151.*.***说if(id<-1)
- **118.113.*.***说多谢lz的分享
- **zsxwing**说你的测试环境是什么呢

订阅

新浪微博

流火枫林

粉丝169人

国内关注RxJava的人太少了。不知道@邓草原 老师能否帮忙多share一些使用经验。
8月14日 09:43

转发了hashjoin 的微博：今天Pivotal宣布了会把整个Spark stack包装在Pivotal HD Hadoop发行版里面。这意味这最大的四个Hadoop发行商（Cloudera, Pivotal, MapR, Hortonworks）都提供了对Spark的支持。http://t.cn/RvLF7aM 星火燎原的开始。
转发理由：转发微博
5月24日 16:57

同时开着eclipse，IDEA，chrome(N>>10个标签)，还有2个虚拟机。感觉8G内存完全不够用啊。。。
5月8日 13:31

Scala在硅谷真是火啊。都出现在电视剧了。硅谷S01E02

更多>>