openssl 非对称加密算法DSA命令详解

1、DSA算法概述

DSA算法是美国的国家标准数字签名算法，它只能用户数字签名，而不能用户数据加密和密钥交换。

DSA与RSA的生成方式不同，RSA是使用openssl提供的指令一次性的生成密钥(包括公钥)，而通常情况下，DSA是先生成DSA的密钥参数，然后根据密钥参数生成DSA密钥(包括公钥)，密钥参数决定了DSA密钥的长度，而且一个密钥参数可以生成多对DSA密钥对。

DSA生成的密钥参数是p、q和g，如果要使用一个DSA密钥，需要首先共享其密钥参数。关于DSA加密的原理，请自行查阅。

2、DSA算法相关指令及用法

openssl中DSA算法指令主要有三个，分别是

指令	功能
dsaparam	生成、处理DSA密钥参数，也可以直接生成DSA密钥
dsa	处理DSA密钥格式的转换
gendsa	根据DSA密钥参数生成一个DSA密钥

从上表可以看到，dsa和gendsa和RSA相关指令中的rsa和genrsa用法相似，但是DSA相关指令中没有提供签名和验证操作的dsautl指令，所以如果需要使用DSA进行签名和验证，需要借助dgst指令，该指令在后续章节中介绍。

2.1 dsaparam指令说明

dsaparam主要用户生成密钥参数，也可以生成DSA密钥其用法如下

```
xlzh@cmos:~/test$ openssl dsaparam -
unknown option -
dsaparam [options] [bits] <infile >outfile
where options are
 -inform arg    input format - DER or PEM                       //
 -outform arg   output format - DER or PEM                      //
 -in arg        input file                                      //
 -out arg       output file                                     //
 -text          print as text                                   //
 -C             Output C code                                   //
 -noout         no output                                       //
 -genkey        generate a DSA key                              //
 -rand          files to use for random number input            //
 -engine e      use engine e, possibly a hardware device.       //
 number         number of bits to use for generating private key   //
xlzh@cmos:~/test$
```

其参数与RSA相关指令的参数类似，不再一一说明，下面以实例的方式说明其用法

1、生成密钥参数并查看其各个参数值

```
/*生成1024位的密钥参数*/
xlzh@cmos:~/test$ openssl dsaparam -out DSAP.pem 1024
Generating DSA parameters, 1024 bit long prime
This could take some time
....
```


< 2020年4月 >

日	一	二	三	四	五	六
29	30	31	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	1	2
3	4	5	6	7	8	9

搜索
找找看
谷歌搜索

常用链接
我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签
android(6)
逆向(4)
Hook(2)
ida(2)
genrsa(2)
RSA(2)
smali(2)
so(1)
sphinx(1)
substrate(1)
更多

随笔分类
android(6)
android安全(11)
C/C++(2)
git(1)
Linux(3)
openssl(8)
Scracpy(2)
Windows(1)
渗透测试
协议(2)

```
/*明文查看密钥参数的值*/
xlzh@cmos:~/test$ openssl dsaparam -in DSAP.pem -text -noout
```

2、密钥参数格式间的转换

```
/*pem格式的密钥参数转为der格式*/
xlzh@cmos:~/test$ openssl dsaparam -in DSAP.pem -out DSAP.der -outform der
/*der格式的密钥参数转为pem格式*/
xlzh@cmos:~/test$ openssl dsaparam -in DSAP.der -inform der -out R_DSAP.pem
xlzh@cmos:~/test$ diff DSAP.pem R_DSAP.pem
```

3、直接生成DSA密钥

```
/*直接生成DSA密钥*/
xlzh@cmos:~/test$ openssl dsaparam -genkey -out DSA.pem 1024
Generating DSA parameters, 1024 bit long prime
...
/*查看DSA密钥，可知参数和密钥都被放在输出文件中，说明本质上还是先生成参数，再利用参数生成密钥*/
xlzh@cmos:~/test$ cat DSA.pem
-----BEGIN DSA PARAMETERS-----
MIIBHgKBgQDAG1CFQRqKgrDa21dT2SO0OtvR0wtKo4GWEH+zikTt6eh6S0CdhtqX
PdPiboZdYAJy7HzKHLe0BUkf4dfOOPZBcQrr9sYkJ6q2Zz/jSSA9EnpuQfstdE8a
2wrhIm8mPzBKuWfvz29O6KlBngLfXSfr8Iy2mNAf7NgAntDBMY8yHQIVAMaCaSge
oBHtVo9cUoA5E69f2VqrAoGAbzC9wFnra1lT8Egak4N7YHkBwObN3T2ue3tRM7wE
uv5rNuIyQrSQnp4vqFcnu3lOrP3ZGEJvE2OkVo7e6LhfO8V0UOqElfhiuwEaZuzZ
22Sodbu7lUx3YMU1QRvk42IudIevi6LWq4zk+sxraAZ3h5rvo8/pKayxtRuKq8Ep
5kU=
-----END DSA PARAMETERS-----
-----BEGIN DSA PRIVATE KEY-----
MIIBugIBAAKBgQDAG1CFQRqKgrDa21dT2SO0OtvR0wtKo4GWEH+zikTt6eh6S0Cd
htqXPdPiboZdYAJy7HzKHLe0BUkf4dfOOPZBcQrr9sYkJ6q2Zz/jSSA9EnpuQfst
dE8a2wrhIm8mPzBKuWfvz29O6KlBngLfXSfr8Iy2mNAf7NgAntDBMY8yHQIVAMaC
aSgeoBHtVo9cUoA5E69f2VqrAoGAbzC9wFnra1lT8Egak4N7YHkBwObN3T2ue3tR
M7wEuv5rNuIyQrSQnp4vqFcnu3lOrP3ZGEJvEZ0kVo7e6LhfO8V0UOqElfhiuwEa
ZuzZ22Sodbu7lUx3YMU1QRvk42IudIevi6LWq4zk+sxraAZ3h5rvo8/pKayxtRuK
q8Ep5kUCgYAh50mq26xMHfVxb/EkZzH+ouM3zPk6x8f9GFZzuUtGfNCzopTxEmw3
yYPaBwiojhZnK/LXVdEui97+D/rqAPCXAfwFhXLR9w7oikid+Ai1A1B+lycCJrim
gyF/dzha7uYGzaA1+rAftE76aeGlZYnoO42CgkxuYsxYxCzTJF8swQIUcrqFkFhN
Z2th/K4MZwy4QW6xPrA=
-----END DSA PRIVATE KEY-----
```

2.1 gendsa指令说明

gendsa指令功能简单，即利用输入的密钥参数生成DSA密钥

```
xlzh@cmos:~/test$ openssl gendsa -
usage: gendsa [args] dsaparam-file
 -out file - output the key to 'file'
 -des      - encrypt the generated key with DES in cbc mode
 -des3     - encrypt the generated key with DES in ede cbc mode (168 bit key)
 -seed
                encrypt PEM output with cbc seed
 -aes128, -aes192, -aes256
                encrypt PEM output with cbc aes
 -camellia128, -camellia192, -camellia256
                encrypt PEM output with cbc camellia
 -engine e - use engine e, possibly a hardware device.
 -rand file:file:...
           - load the file (or the files in the directory) into
             the random number generator
 dsaparam-file
           - a DSA parameter file as generated by the dsaparam command
```

示例如下：

1、根据密钥参数生成密钥

```
/*根据密钥参数生成密钥*/
xlzh@cmos:~/test$ openssl gendsa -out DSA1.pem  DSAP.pem
Generating DSA key, 1024 bits
```


最新评论

1. Re:openssl 对称加密算法enc命令详解
fedora 29 x86 workstation OpenSSL 1.1.1d FIPS 10 Sep 2019 没有 aes-256-gcm. openssl enc -ciphers 何解...
--NickD
2. Re:openssl 对称加密算法enc命令详解
-pass env:passwd 的passwd的前面不需要加$ ？
--creazyloser
3. Re:Android AccessibilityService(辅助服务) 使用示例
他是返回的整个activity 的view ，所以会包含三个Fragment 的
--伍歌歌
4. Re:PPTP协议握手流程分析
大佬 自己能用软件模拟vpn 并建立通道 进行数据传输吗
--54辉哥
5. Re:Https协议简析及中间人攻击原理
写的不错
--aqu415

```
xlzh@cmos:~/test$ openssl gendsa -out DSA2.pem  DSAP.pem
Generating DSA key, 1024 bits
/*相同密钥参数，每次生成的密钥不同*/
xlzh@cmos:~/test$ diff DSA1.pem DSA2.pem
8,11c8,11
< TWcw1+XFAoGAEA1DLnv5efzB+ipIQ29q0ZedLVPyxdB44jpZES+esBQtU04HdI2N
< bClgwj8c9M6Y/9rL1uy3NqKaGHM+mjLyAXVceigFx7v15r5LRmWjialdqkcVG/3S
< Qo530ui/tXgFbFV9iA6C8L+nHDMPOf5v6oGyICmxN8DWzhQAsmy9mkICFBeqMbZM
< 9qBeG0BaS/6PucBxObsv
---
> TWcw1+XFAoGALWkjJeFunfvkiarJ1/pw8Lqvuyu/Glt3g/hURPPlrOIhA0pFXDmC
> UzCM1x6wrHWFc0jmUNk6FtnjGyiCLxVJGzeB7/4MA35aInHkiHwzX7a+B0At8bMq
> WEkWtzxhvTxTqWTAcC02Qr2mNNfJwWWVV0jVzMtm3Gb6YwhNnUvxp0ACFHrXO/8h
> dIwr6pSuj6vdNpHFDlY2
/*生成密钥并使用des3加密存储*/
xlzh@cmos:~/test$ openssl gendsa -out DSA.pem -des3 -passout pass:123456 DSAP.pem
Generating DSA key, 1024 bits
```

2.1 dsa指令说明

dsa和rsa指令功能及其类似，如下

```
xlzh@cmos:~/test$ openssl dsa -
unknown option -
dsa [options] <infile >outfile
where options are
 -inform arg     input format - DER or PEM
 -outform arg    output format - DER or PEM
 -in arg         input file
 -passin arg     input file pass phrase source
 -out arg        output file
 -passout arg    output file pass phrase source
 -engine e       use engine e, possibly a hardware device.
 -des            encrypt PEM output with cbc des
 -des3           encrypt PEM output with ede cbc des using 168 bit key
 -aes128, -aes192, -aes256
                 encrypt PEM output with cbc aes
 -camellia128, -camellia192, -camellia256
                 encrypt PEM output with cbc camellia
 -seed           encrypt PEM output with cbc seed
 -text           print the key in text
 -noout          don't print key out
 -modulus        print the DSA public value
```

示例如下：

1、加密密钥和解密密钥

```
/*生成未加密的DSA密钥*/
xlzh@cmos:~/test$ openssl dsaparam -out DSA.pem -genkey 1024
/*使用des3加密DSA密钥*/
xlzh@cmos:~/test$ openssl dsa -in DSA.pem -out E_DSA.pem -des3 -passout pass:123456
read DSA key
writing DSA key
/*解密DSA密钥*/
xlzh@cmos:~/test$ openssl dsa -in E_DSA.pem -out DSA1.pem -passin pass:123456
read DSA key
writing DSA key
```

2、提取DSA的公钥

```
xlzh@cmos:~/test$ openssl dsa -in DSA.pem -out pub.pem -pubout
read DSA key
writing DSA key
```

3、小结

可以看到，DSA和RSA的指令非常相似，熟悉了其中一种，另外一种也很容易上手。而且openssl提供的指令虽多，但参数来来回回就那么多，在多数情况下不同指令的相同参数含义大概一样。

到此为止，介绍了对称加密算法指令，非对称加密算法RSA和DSA相关指令，这些都是一些基础指令，在实际应用中，我们使用openssl做的大多数是与CA有关的签名、验证、加密、解密等。所以接下来要写的是和实际应用相关的内容，比如证书自签名、二级证书签发、终端证书签发、证书验证等内容。

分类: openssl

标签: DSA, 密钥参数, openssl, RSA, genrsa, rsaparam

Gordon0918
关注 - 1
粉丝 - 21
+加关注

0 0

« 上一篇: openssl 非对称加密算法RSA命令详解
» 下一篇: openssl 摘要和签名验证指令dgst使用详解

posted @ 2016-04-08 17:11 Gordon0918 阅读(4334) 评论(1) 编辑 收藏

评论

#1楼 2016-04-08 18:04 | 花儿笑弯了腰

谢谢分享!

支持(0) 反对(0)

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册， 访问 网站首页。

相关博文:
· openssl 非对称加密算法RSA命令详解
· 非对称加密过程详解（基于RSA非对称加密算法实现）
· openssl用法详解
· 各种加密算法比较
· OpenSSL Command-Line HOWTO
» 更多推荐...

最新 IT 新闻:
· 再发十款新品后，苏宁小Biu离全屋智能还有多远?
· 英伟达、强生的 AI 招聘神器，如何把招人效率提高四成?
· Google Cloud 发布 COVID-19 数据集，可构建 AI 模型来对抗疫情
· 程序员的一次失误，在 45 分钟里搞垮了一家上市公司
· 这一次，绝大多数的远程办公会失败
» 更多新闻...