首先说一下，buu上的题目应该是没问题的

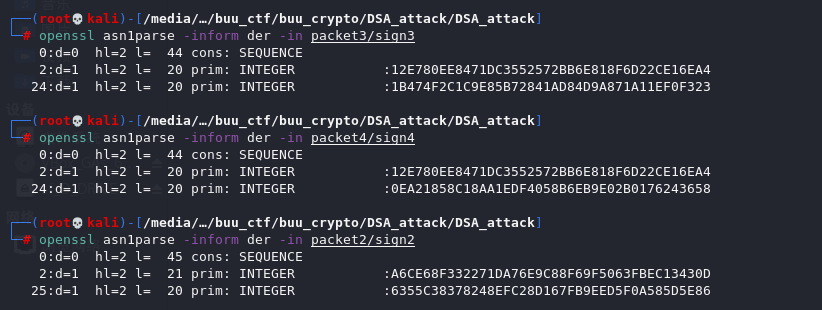
主要是先看到ctf wiki和[Jarvis's Blog](https://www.jarvisw.com/)先入为主地觉得buu上的题packet里的签名也改过，因为通过截图可以看出packet4和3里的签名和文章中验证错误的一样，就以为有问题，去[Jarvis's Blog](https://www.jarvisw.com/)博客的oj网站找修复题结果注册了登不上去，已经在Jarvis师傅博客下留言了希望及时修复吧，然后就按wiki上的exp复现了一下，当然得不到flag，s3，s4和r都不一样，本来打算关文件夹结束了都突然想自己校验一下，用buu上文件都s3，s4和r试一下，结果flag正确，校验packet4也正确，所以buu上的应该就是源文件，且是正确无误的。

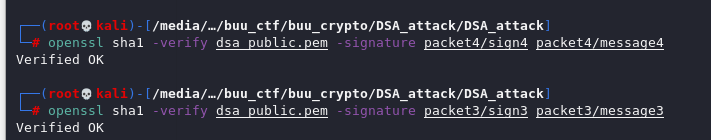
参考

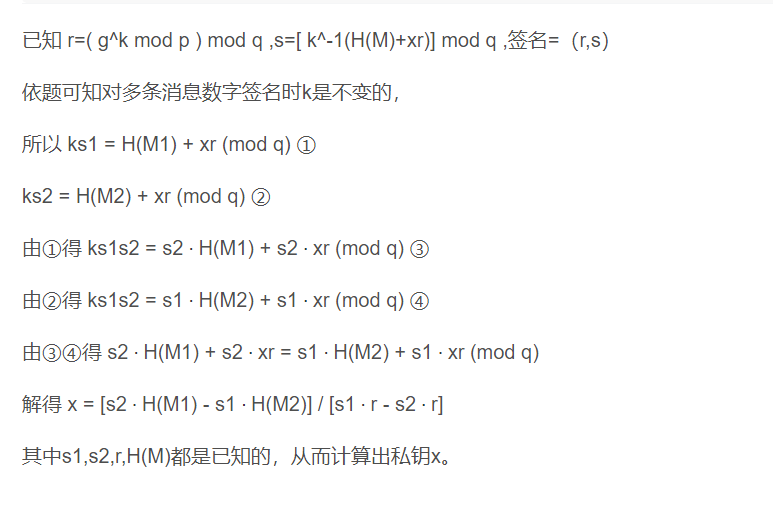
<https://www.jarvisw.com/?p=169>

<https://ctf-wiki.org/crypto/signature/dsa/#k_1>

<https://blog.csdn.net/qq_35964497/article/details/78984733>







<https://blog.csdn.net/jiftlixu/article/details/19329893>

openssl简单使用



用法：openssl asn1parse [-inform PEM|DER] [-in filename] [-out filename]

[-noout] [-offset number] [-length number] [-i] [- structure filename]    
  
[-strparse offset]    
  
用途：一个诊断工具，可以对ASN1结构的东东进行分析。    
ASN1是什么？一个用来描述对象的标准。要解释的话，文章可以比解释openssl结构的文章更长。有兴趣的话自己去网络上找来看吧。    
  
-inform DER|PEM|TXT    
输入的格式，DER是二进制格式，PEM是base64编码格式,TXT不用解释了吧    
  
-in filename    
输入文件的名称，缺省为标准输入。    
  
-out filename    
输入文件的名称，输入一般都是DER数据。如果没这个项，就没有东西输入咯。该项一般都要和-strparse一起使用。    
  
-noout    
不要输出任何东西(不明白有什么用)    
  
-offset number    
从文件的那里开始分析，看到offset就应该知道是什么意思了吧。    
  
-length number    
一共分析输入文件的长度的多少，缺省是一直分析到文件结束。    
  
-i    
根据输出的数据自动缩进。    
  
- structure filename    
当你输入的文件包含有附加的对象标志符的时候，使用这个。    
这种文件的格式在后面会介绍。    
  
-strparse offset    
从由offset指定的偏移量开始分析ASN1对象。当你碰到一个嵌套的对象时，可以反复使用这个项来一直进到里面的结构捏出你需要的东东。    
一般分析完之后输入的东东如下：    
openssl asn1parse -out temp.ans -i -inform pem < server.crt    
  
0:d=0 hl=4 l= 881 cons: SEQUENCE    
  
4:d=1 hl=4 l= 730 cons: SEQUENCE    
  
... ....    
  
172:d=3 hl=2 l= 13 prim: UTCTIME :000830074155Z    
  
187:d=3 hl=2 l= 13 prim: UTCTIME :010830074155Z    
  
202:d=2 hl=3 l= 136 cons: SEQUENCE    
  
205:d=3 hl=2 l= 11 cons: SET    
  
... ...    
  
359:d=3 hl=3 l= 141 prim: BIT STRING    
  
... ...    
本例是一个自签名的证书。每一行的开始是对象在文件里的偏移量。d=xx是结构嵌套的深度。知道ASN1结构的人应该知道，每一个SET或者SEQUENCE都会让嵌套深度增加1.    
hl=xx表示当前类型的header的长度。1=xx表示内容的八进制的长度。    
-i可以让输出的东西容易懂一点。    
如果没有ASN.1的知识，可以省略看这一章。    
本例中359行就是证书里的公共密钥。可以用-strparse来看看    
openssl asn1parse -out temp.ans -i -inform pem -strparse 359 < server.crt    
  
0:d=0 hl=3 l= 137 cons: SEQUENCE    
  
3:d=1 hl=3 l= 129 prim: INTEGER :C0D802B4C084B20569C619C0FDF    
  
466EEB7980920A408D51DA22C20427AC32488665D931C41E3274912DE2F25C8CA9C97B75    
  
415C01794B622DBEADD92DA068C140C3AD387BF5FDC9A8D2FCEE7F7F3E36B0194994FD67    
  
07897C8969F16F6ECB3F03BF985E910817160FE5DCBF874B1C0DBD06A568E130DA7C9FE3    
  
9FE7A7F421369    
  
135:d=1 hl=2 l= 3 prim: INTEGER :010001    
不要试图去看temp.ans的内容，是二进制来的，看不懂的。