XCTF密码学（入门二）

原创

[牛奶糖不甜](#) 于 2020-10-25 23:54:30 发布 323 收藏

分类专栏： [XCTF：crypto（入门）](#)

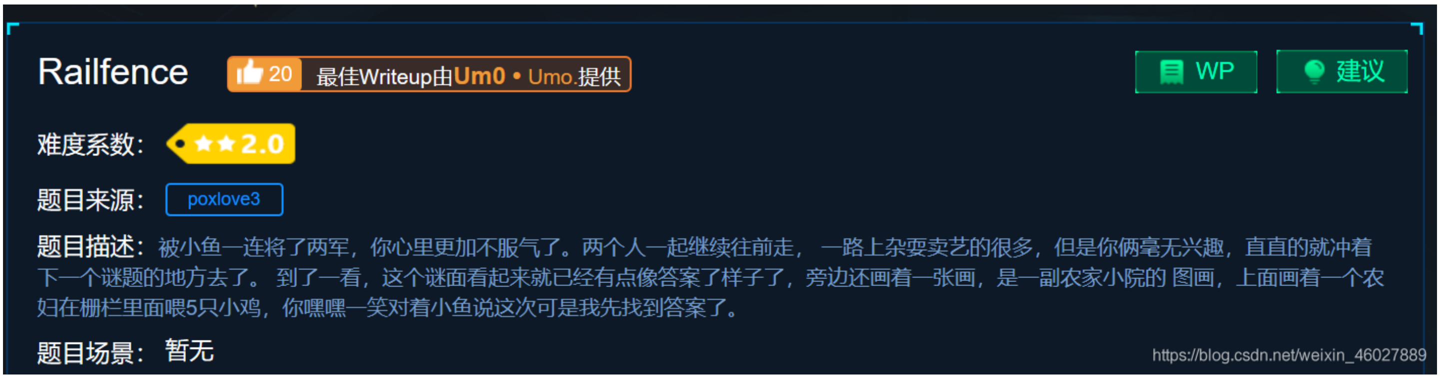
本文链接：https://blog.csdn.net/weixin_46027889/article/details/109121873

XCTF密码学（入门二）

5.1题目：Railfence

5.2描述：被小鱼一连将了两军，你心里更加不服气了。两个人一起继续往前走， 一路上杂耍卖艺的很多，但是你俩毫无兴趣，直直的就冲着下一个谜题的地方去了。 到了一看，这个谜面看起来就已经有点像答案了样子了，旁边还画着一张画，是一副农家小院的 图画，上面画着一个农妇在栅栏里面喂5只小鸡，你嘿嘿一笑对着小鱼说这次可是我先找到答案了。

5.3附件：ccehgyaefnpeoobe{lcirg}epriec_ora_g



Railfence 最佳Writeup由Um0 • Umo.提供

难度系数：2.0

题目来源：poxlove3

题目描述：被小鱼一连将了两军，你心里更加不服气了。两个人一起继续往前走， 一路上杂耍卖艺的很多，但是你俩毫无兴趣，直直的就冲着下一个谜题的地方去了。 到了一看，这个谜面看起来就已经有点像答案了样子了，旁边还画着一张画，是一副农家小院的 图画，上面画着一个农妇在栅栏里面喂5只小鸡，你嘿嘿一笑对着小鱼说这次可是我先找到答案了。

题目场景： 暂无

https://blog.csdn.net/weixin_46027889

题目Railfence翻译过来是栏杆的意思，于是我们知道这是栅栏密码。

直接用在线工具解密地址：http://www.atoolbox.net/Tool.php?Id=855

由题目的五只小鸡知道是5个一组，结果得到cyperrocae{gireeol}eahfocec_gnbip_g这串乱码，忽然想到栅栏密码还有一种叫w的变种，解密机制如下所示。

先将字符按照下面的方式排列。

```
c        c        e          h         g
 y      a e       f n       p e       o  o
  b    e   {     l   c    i     r    g    {
   e  p     r   i     e  c       -  o
     r        a        -          g
```

接着按从上到下从左到右的顺序读取，得到flag

也可以用在线工具解密

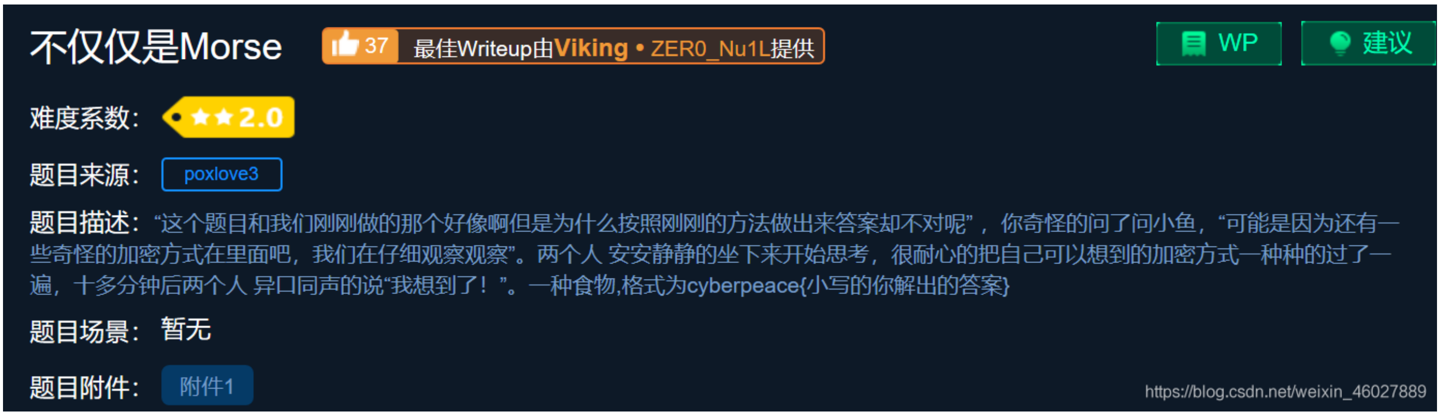
http://www.atoolbox.net/Tool.php?Id=777

6.1题目：不仅仅是Morse

6.2描述：“这个题目和我们刚刚做的那个好像啊但是为什么按照刚刚的方法做出来答案却不对呢”，你奇怪的问了问小鱼，“可能是因为还有一些奇怪的加密方式在里面吧，我们在仔细观察观察”。两个人 安安静静的坐下来开始思考，很耐心的把自己可以想

到的加密方式一种种的过了一遍，十多分钟后两个人 异口同声的说"我想到了！"。一种食物,格式为cyberpeace{小写的你解出的答案}

6.3附件：–/.-/-.–/…–.-/-…/./…–.-/…/.-/…-/./…–.-/.-/-./—/-/…/./.-./…–.-/-…/./-.-./—/-…/./…/…/…/…/.-/.-/.-/.-/.-/-…/.-/.-/-…/-…/-…/.-/.-/-…/-…/.-/.-/.-/.-/.-/.-/.-/.-/-…/.-/.-/-…/.-/-…/.-/.-/.-/.-/.-/.-/.-/-…/-…/.-/-…/.-/.-/.-/-…/-…/.-/.-/.-/-…/-…/.-/-…/.-/.-/.-/.-/-…/.-/-…/.-/.-/-…/.-/.-/.-/-…/-…/.-/-…/.-/.-/.-/-…/.-/.-/.-/-…/.-/.-/-…/.-/-…/-…/.-/.-/-…/-…/-…/.-/-…/.-/.-/.-/-…/.-/-…/.-/-…/-…/.-/.-/.-/-…/-…/.-/-…/.-/.-/.-/-…/.-/.-/-…/.-/.-/.-/.-/-…/-…/.-/-…/-…/.-/.-/-…/-…/.-/.-/-…/.-/.-/-…/.-/.-/.-/-…/.-/.-/-…/.-/.-/-…/.-/.-/-…/.-/-…/.-/.-/-…/-…/.-/-…/.-/.-/.-/.-/-…/-…/.-/-…/.-/-…/-…/.-



不仅仅是Morse 37 最佳Writeup由**Viking** • ZER0_Nu1L提供

难度系数：★★2.0

题目来源：poxlove3

题目描述："这个题目和我们刚刚做的那个好像啊但是为什么按照刚刚的方法做出来答案却不对呢"，你奇怪的问了问小鱼，"可能是因为还有一些奇怪的加密方式在里面吧，我们在仔细观察观察"。两个人 安安静静的坐下来开始思考，很耐心的把自己可以想到的加密方式一种种的过了一遍，十多分钟后两个人 异口同声的说"我想到了！"。一种食物,格式为cyberpeace{小写的你解出的答案}

题目场景：暂无

题目附件：附件1

https://blog.csdn.net/weixin_46027889

首先将附件里的内容去掉"/"以摩斯密码解密出来:

may_be_have_another_decodehhhhaaaaabaabbbaabbaaaaaaaaaabaabababaaaaaaabbabaaabbaaabbaabaaaababaabaaabbabaaabaaabaababbaabbbabaaababababbaaabbabaaabaabaaaabbabbaabbaabaabaaabaabaabaabaaaababaabbabaaaabbabaabba

摩斯：http://ctf.ssleye.com/morse.html

发现还有一层加密，题目说是食物，猜测是培根密码得到attackanddefenceworldisinteresting

提交（注意题目要求）

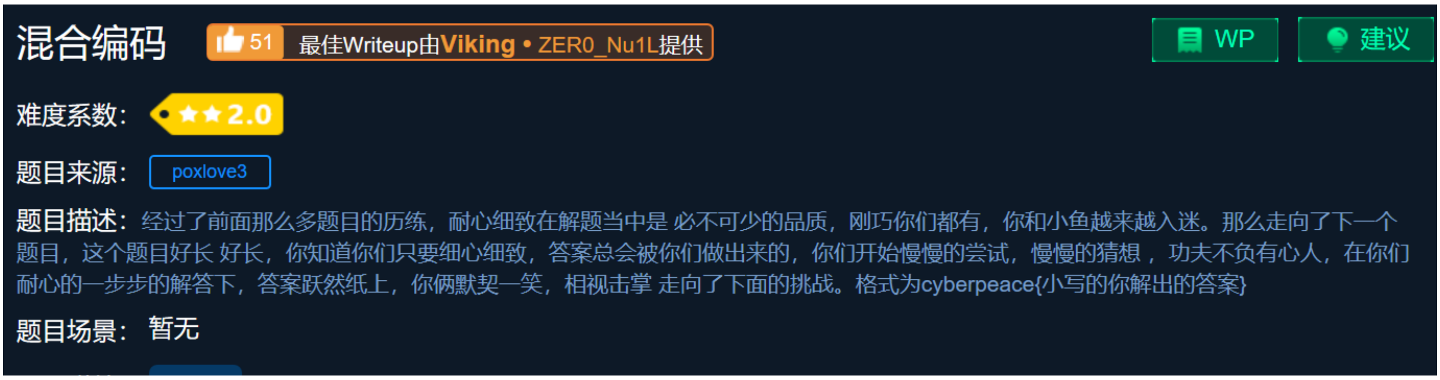
培根：http://ctf.ssleye.com/baconian.html

7.1题目：混合编码

7.2描述：经过了前面那么多题目的历练，耐心细致在解题当中是 必不可少的品质，刚巧你们都有，你和小鱼越来越入迷。那么走向了下一个题目，这个题目好长 好长，你知道你们只要细心细致，答案总会被你们做出来的，你们开始慢慢的尝试，慢慢的猜想 ，功夫不负有心人，在你们耐心的一步步的解答下，答案跃然纸上，你俩默契一笑，相视击掌 走向了下面的挑战。格式为cyberpeace{小写的你解出的答案}

7.3附件：

JiM3NjsmIzEyMjsmIzY5OyYjMTIwOyYjNzk7JiM4MzsmIzU2OyYjMTIwOyYjNzc7JiM2ODsmIzY5OyYjMTE4OyYjNzc7JiM4NDsmIzY1OyYjNTI7JiM3NjsmIzEyMjsmIzEwNzsmIzUzOyYjNzY7JiMxMjI7JiM2OTsmIzEyMDsmIzc3OyYjODM7JiM1NjsmIzEyMDsmIzc3OyYjNjg7JiMxMDc7JiMxMTg7JiM3NzsmIzg0OyYjNjU7JiMxMjA7JiM3NjsmIzEyMjsmIzY5OyYjMTIwOyYjNzg7JiMxMDU7JiM1NjsmIzEyMDsmIzc3OyYjODQ7JiM2OTsmIzExODsmIzc5OyYjODQ7JiM5OTsmIzExODsmIzc3OyYjODQ7JiM2OTsmIzExOTsmIzc3OyYjNzc7JiMxMjI7JiM2OTsmIzEwODsmIzc1OyYjNTY7JiM1MzsmIzc1OyYjNTY7JiMxMDE7JiM4MzsmIzExOTsmIzc3OyYjNjg7JiM4NDsmIzY5OyYjMTE4OyYjNzc7JiMxMjE7JiM2OTsmIzEyMjsmIzY2OyYjMTE0OyYjNzc7JiM3NzsmIzY5OyYjNzg7JiM2OTsmIzEyMDsmIzc3OyYjMTE5OyYjODQ7JiM2NzsmIzc4OyYjMTE4OyYjNzY7JiMxMjI7JiM2OTsmIzExOTsmIzc3OyYjNjc7JiM3NjsmIzEyMjsmIzY5OyYjMTIyOyYjNjY7JiMxMDc7JiM4MjsmIzUxOyYjMTIyOyYjNzc7JiMxMDc7JiM4NDsmIzEwNzsmIzEyMDsmIzY5OyYjMTE5OyYjNzc7JiM4NzsmIzY5OyYjMTE4OyYjNzg7JiM2OTsmIzExODsmIzc4OyYjNjk7JiMxMTk7JiM3NzsmIzY3OyYjNzY7JiMxMjI7JiM2OTsmIzExOTsmIzc3OyYjODQ7JiM2OTsmIzExOTsmIzc3OyYjMTA3OyYjMTE4OyYjNzc7JiMxMjI7JiM5OTsmIzEwNzsmIzc2OyYjNjY7JiMxMDc7JiM4NDsmIzEwNzsmIzEyMDsmIzc3OyYjMTE5OyYjNzc7JiM4NDsmIzY5OyYjMTE5OyYjNzc7JiMxMDc7JiMxMTg7JiM3NzsmIzEyMjsmIzk5OyYjMTA3OyYjMTE4OyYjNzc7JiMxMjI7JiM4OTsmIzEyMDsmIzc3OyYjNjg7JiM1NzsmIzUzOyYjNzY7JiMxMjI7JiM2OTsmIzEyMDsmIzc3OyYjNjc7JiMxMDc7JiMxMTg7JiM3NzsmIzg0OyYjNjk7JiM1MjsmIzc3OyYjODQ7JiM2NjsmIzExOTsmIzc3OyYjODQ7JiM1NjsmIzExODsmIzc3OyYjODQ7JiM2OTsmIzExOTsmIzc3OyYjODQ7JiM2OTsmIzExOTsmIzY5OyYjODQ7JiM5OTsmIzY3OyYjODQ7JiMxMDU7JiM2OTsmIzc3OyYjNjg7JiM4MjsmIzExOTsmIzc3OyYjODQ7JiM5OTsmIzExODsmIzc4OyYjODQ7JiMxMDU7JiM2OTsmIzc3OyYjNjg7JiM2OTsmIzExOTsmIzc3OyYjODQ7JiM2OTsmIzExOTsmIzY5OyYjODQ7JiM5OTsmIzY3OyYjODQ7JiMxMDc7JiM2OTsmIzc3OyYjODQ7JiM2OTsmIzExODsmIzc4OyYjODQ7JiM1NzsmIzExOTsmIzc3OyYjNzc7JiM2OTsmIzU1OyYjNzc7JiMxMjI7JiM5OTsmIzEwNzsmIzc2OyYjNjY7JiMxMDc7JiMxMTg7JiM3NzsmIzEyMjsmIzY5OyYjMTE4OyYjNzc7JiM4NDsmIzk5OyYjMTE4OyYjNzc7JiM4NDsmIzY5OyYjMTE5OyYjNzc7JiM4NDsmIzY5OyYjMTE5OyYjNzc7JiM4NDsmIzY5OyYjMTE5OyYjNjk7JiM4NDsmIzEwNzsmIzc2OyYjNjY7JiMxMDc7JiMxMjA7JiM3NzsmIzExOTsmIzc3OyYjODQ7JiM2OTsmIzExODsmIzY5OyYjODQ7JiM5OTsmIzExODsmIzc3OyYjNjg7JiM2OTsmIzU1OyYjNzc7JiMxMjI7JiM1NzsmIzUzOyYjNzY7JiMxMjI7JiM2OTsmIzExOTsmIzc3OyYjNjg7JiMxMDc7JiMxMjA7JiM3NzsmIzY5OyYjNTU7JiM3NzsmIzg0OyYjMTA3OyYjNzY7



混合编码 51 最佳Writeup由**Viking** • ZER0_Nu1L提供

难度系数：★★2.0

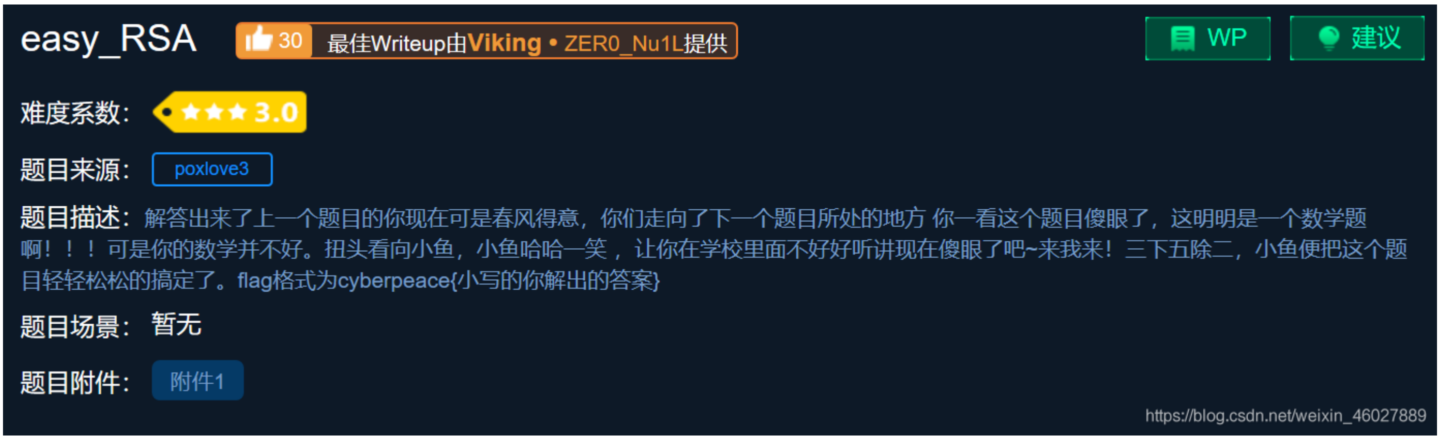
题目来源：poxlove3

题目描述：经过了前面那么多题目的历练，耐心细致在解题当中是 必不可少的品质，刚巧你们都有，你和小鱼越来越入迷。那么走向了下一个题目，这个题目好长 好长，你知道你们只要细心细致，答案总会被你们做出来的，你们开始慢慢的尝试，慢慢的猜想 ，功夫不负有心人，在你们耐心的一步步的解答下，答案跃然纸上，你俩默契一笑，相视击掌 走向了下面的挑战。格式为cyberpeace{小写的你解出的答案}

题目场景：暂无


题目附件：

一看到后面的两个“=”号，base64计算，是unicode的HEX编码，解码后感觉还是base64，再解码得到/119/101/108/99/111/109/101/116/111/97/116/116/97/99/107/97/110/100/100/101/102/101/110/99/101/119/111/114/108/100
很明显是askii码，替换得到flag。
8.1题目：easy_RSA
8.2描述：解答出来了上一个题目的你现在可是春风得意，你们走向了下一个题目所处的地方 你一看这个题目傻眼了，这明明是一个数学题啊！！！可是你的数学并不好。扭头看向小鱼，小鱼哈哈一笑 ，让你在学校里面不好好听讲现在傻眼了吧~来我来！三下五除二，小鱼便把这个题目轻轻松松的搞定了。flag格式为cyberpeace{小写的你解出的答案}
8.3附件：在一次RSA密钥对生成中，假设p=473398607161，q=4511491，e=17
求解出d


easy_RSA

难度系数：3.0

题目来源：poxlove3

题目描述：解答出来了上一个题目的你现在可是春风得意，你们走向了下一个题目所处的地方 你一看这个题目傻眼了，这明明是一个数学题啊！！！可是你的数学并不好。扭头看向小鱼，小鱼哈哈一笑 ，让你在学校里面不好好听讲现在傻眼了吧~来我来！三下五除二，小鱼便把这个题目轻轻松松的搞定了。flag格式为cyberpeace{小写的你解出的答案}

题目场景：暂无

题目附件：附件1

rsa算法都清楚，e的d次方等于n也等于（p-1）*（q-1），求解出的结果d就是flag的内容，因为代码不具备普适性，就先不展示了，有需求在评论区发出来，我下一次补上。