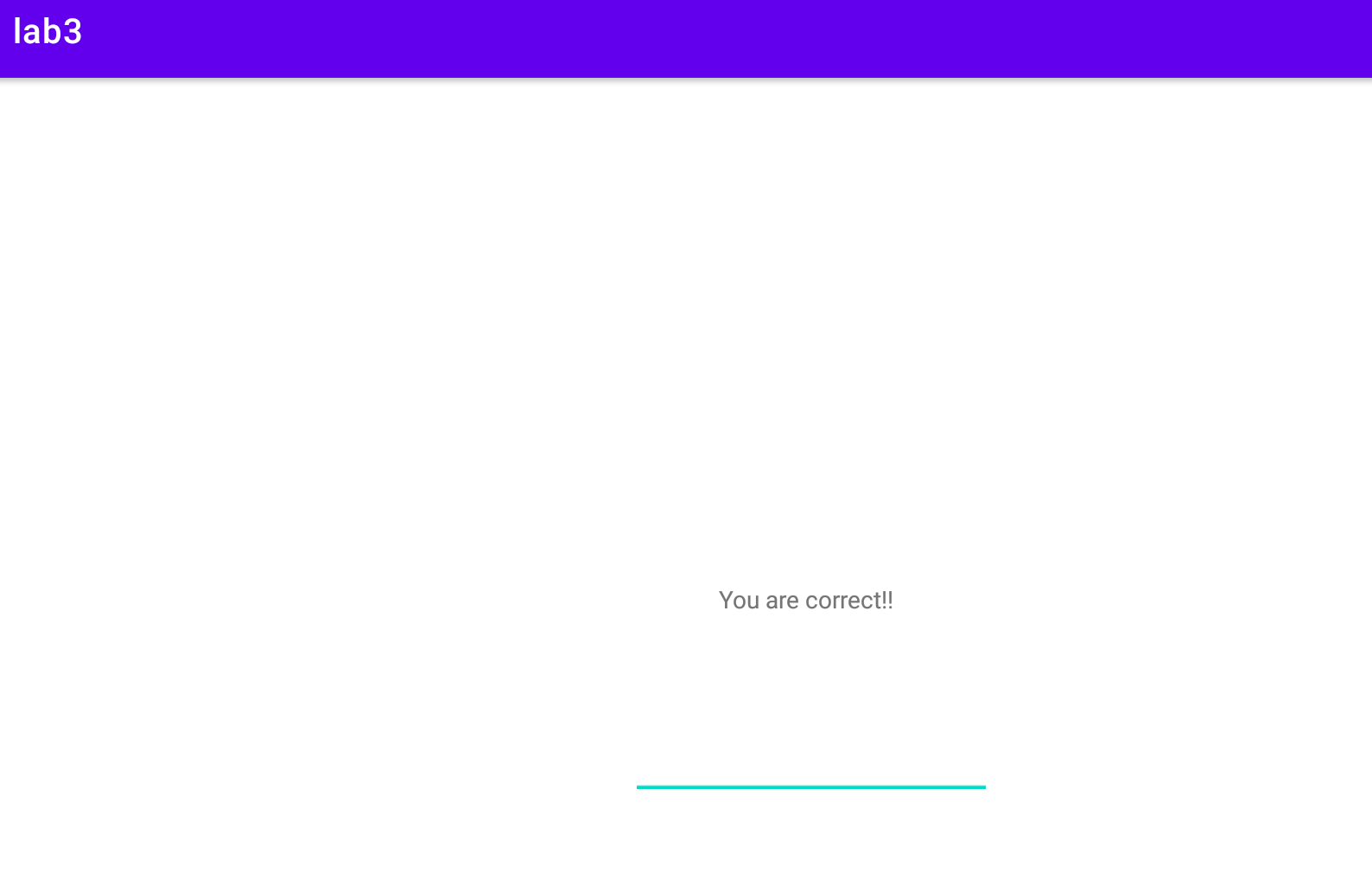
**Lab 3. Deobfuscate Android Apps**

* **Task A**

(1) Your Answer

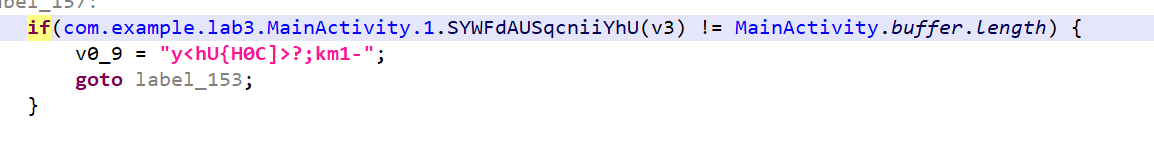
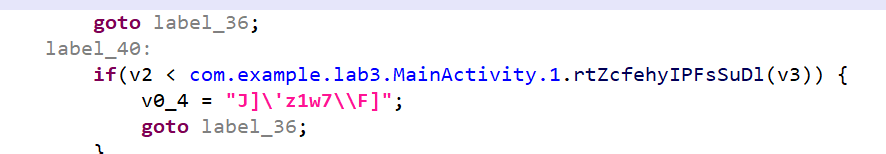
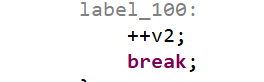
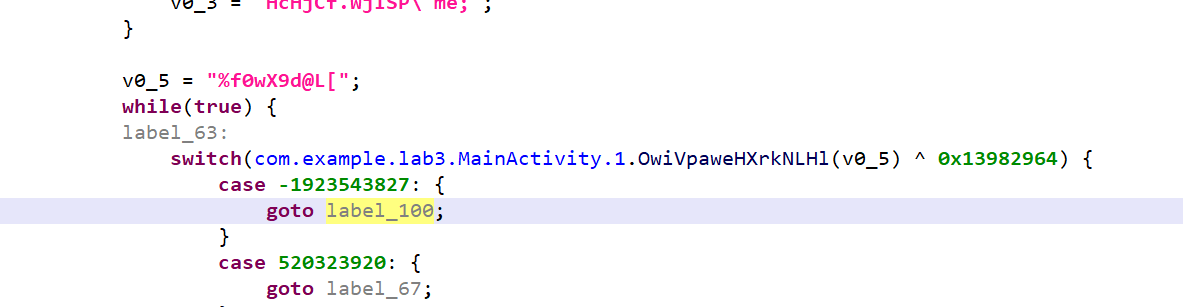
**答案：null（啥都不输入）**



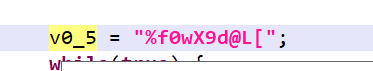
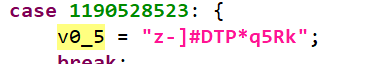
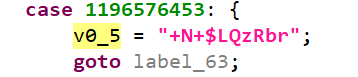
(2) Writeup

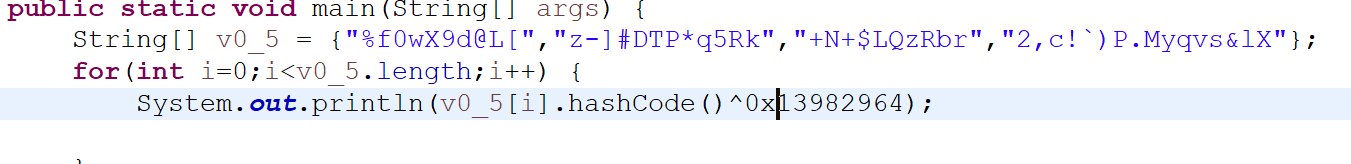
[Record how you solve this task here.]

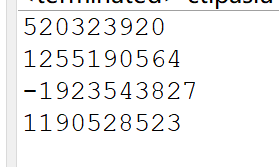
两个方法：

1. 推测：
   1. 关于输入文本有三个条件的判断，其中两个是关于其长度的。
      1. 第一个是判断是否v3.length等于buffer.length
         1. If(true),那么goto label\_153,而这个也是通过label\_153入口进入的——“又回去了”，推测条件是false；
      2. 第二个判断是判断v3.length是否>v2, 此时v2=0;
         1. 
         2. 同第一个的分析，If(true),那么goto label\_36,而这个也是通过label\_36入口进入的——“又回去了”，推测条件是false。
            1. 得出v3==null；
         3. 如果条件是true的话。那么需要进入label\_100来让v2++；
            1. 而label\_100的唯一入口是

仅需验证一下所有v0\_5的值是否能进入label\_100即可。总共有4种。

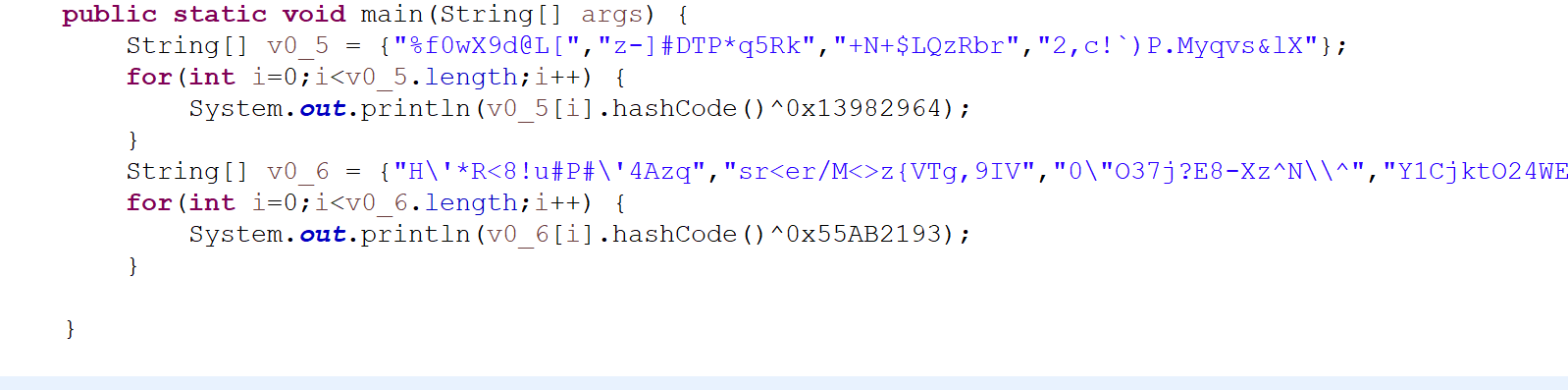
     



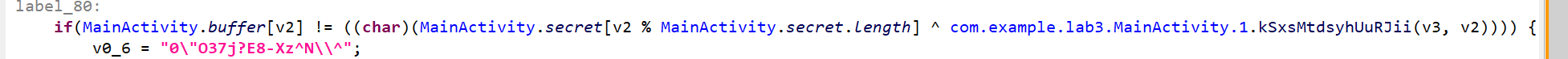


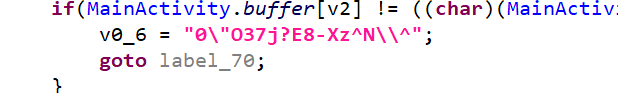
假设失败，有可能进入。进一步分析v2

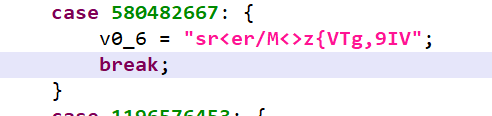
用java计算v0\_6 

可得顺序是先进入label\_80判断（v2=0），因为v3[0]计算出来是ascii码的23——不可打印字符，所以会进入if语句

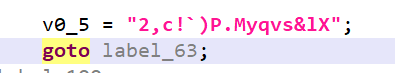


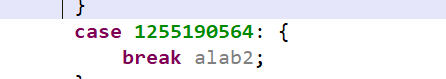


接下来的顺序是label\_70——>

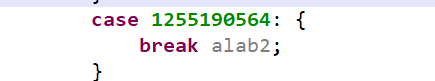
——>

——>

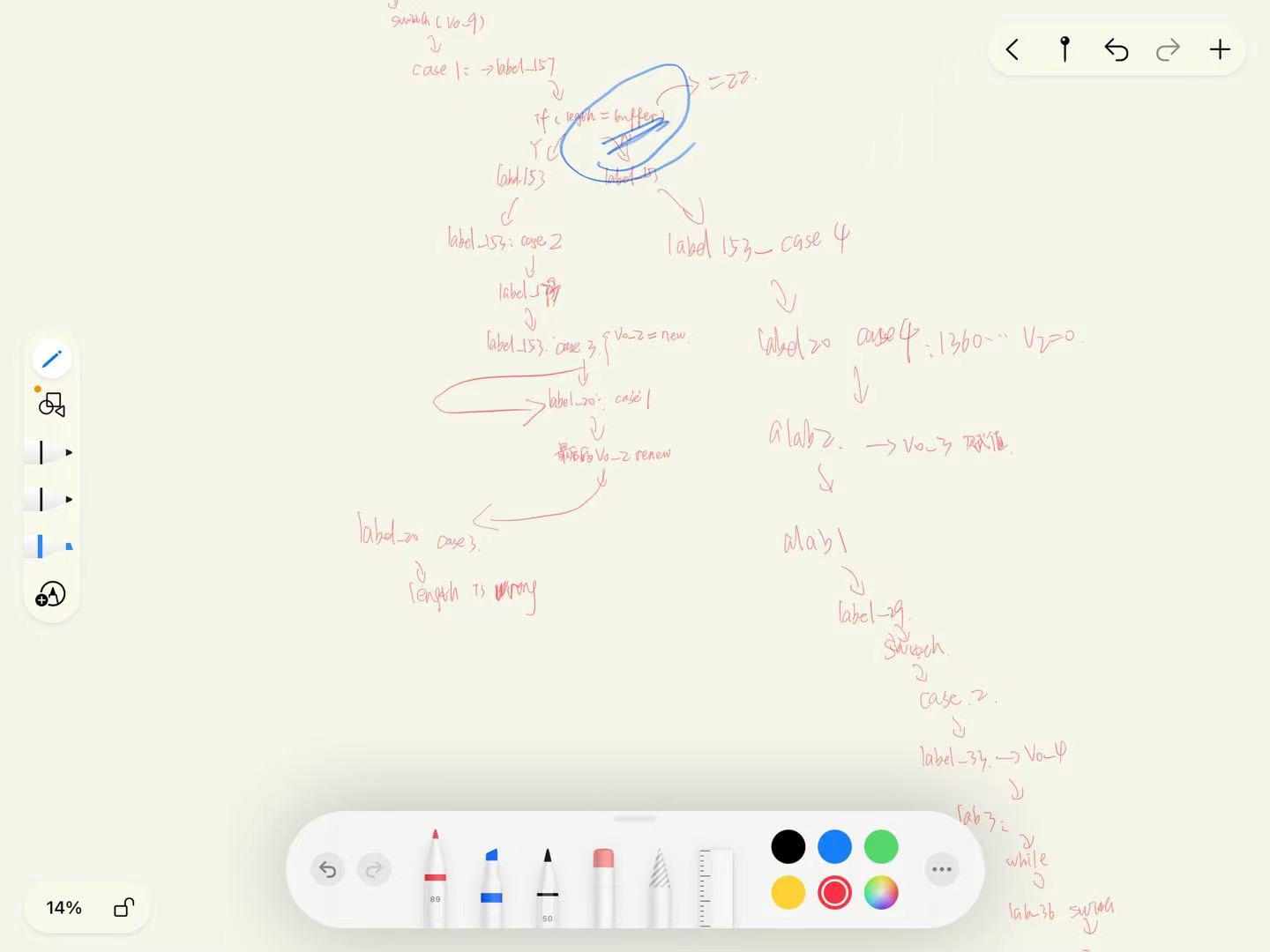
——>

——>

在alab2外部v0\_5只有"z-]#DTP\*q5Rk"——>

如果有机会再进入label\_63，v0\_5也只可能是"z-]#DTP\*q5Rk"，因此再进去也只有一种结果。所以不可能会进入label\_100,v2只能是0；

所以只有v3=null一种情况。

1. 方法二：按顺序逐层推理。
   1. 利用java计算出所有可能的hashcode，进入循环一层一层分析。以下是顺序分析过程的部分。
      1. 

**Task B**

(1) Your Answer

顺序是：

2D858B227616E6FFAC53B2A4BA918B5F

4DBDE00A61FEF8AC53AF420F6ABC7A1A

07F1393D405F0A1A6D951A19428B9DDB

6F9BFC9AE52562A2139CCDE94A2365F3

decrypted string1 : **alarm**

decrypted string2 : **74fc5b28-65e1-4c76-aa5e-bd9c0c44ea01**

decrypted string3: **null (啥也没有)**

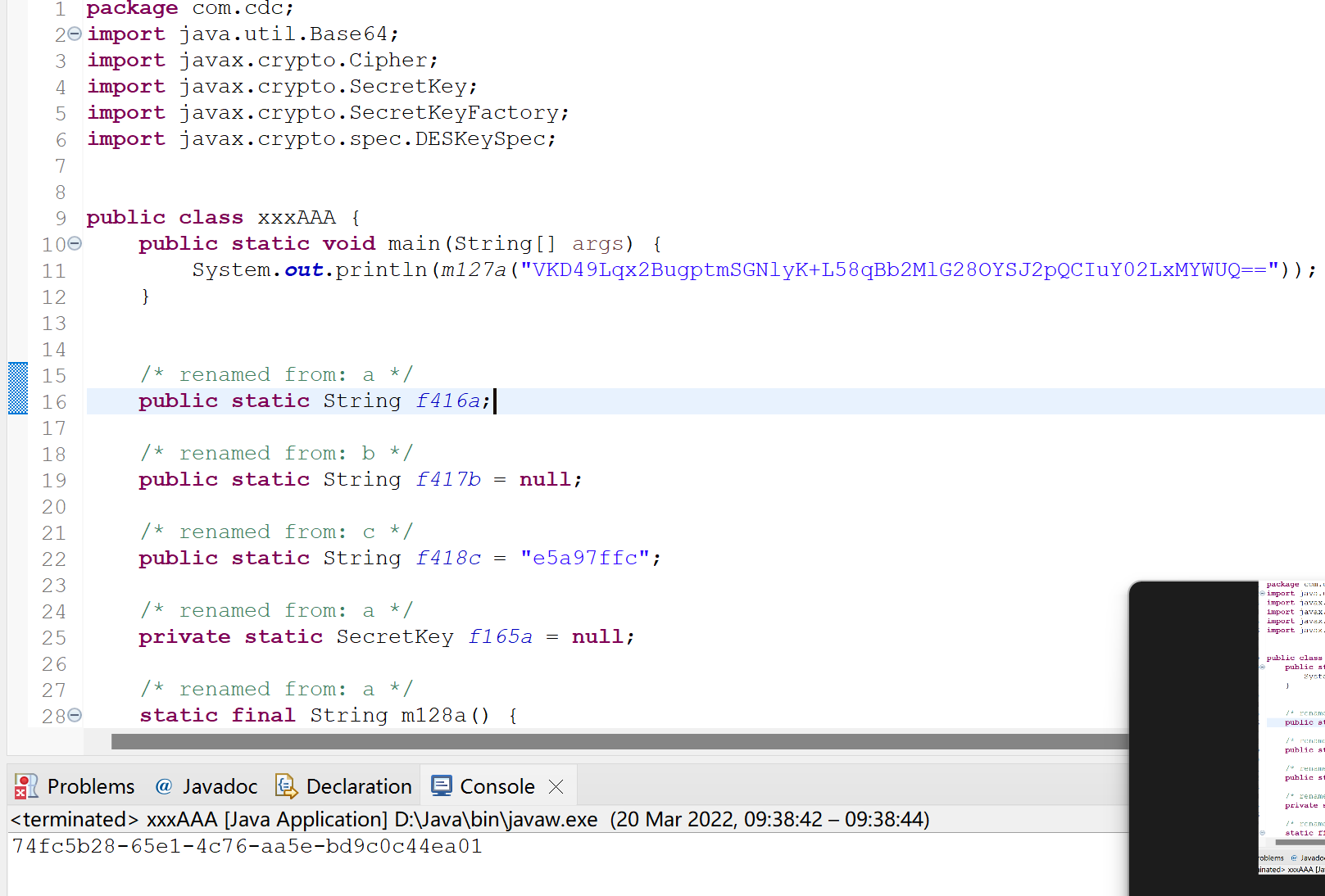
decrypted string4 :  **android.app.extra.DEVICE\_ADMIN**

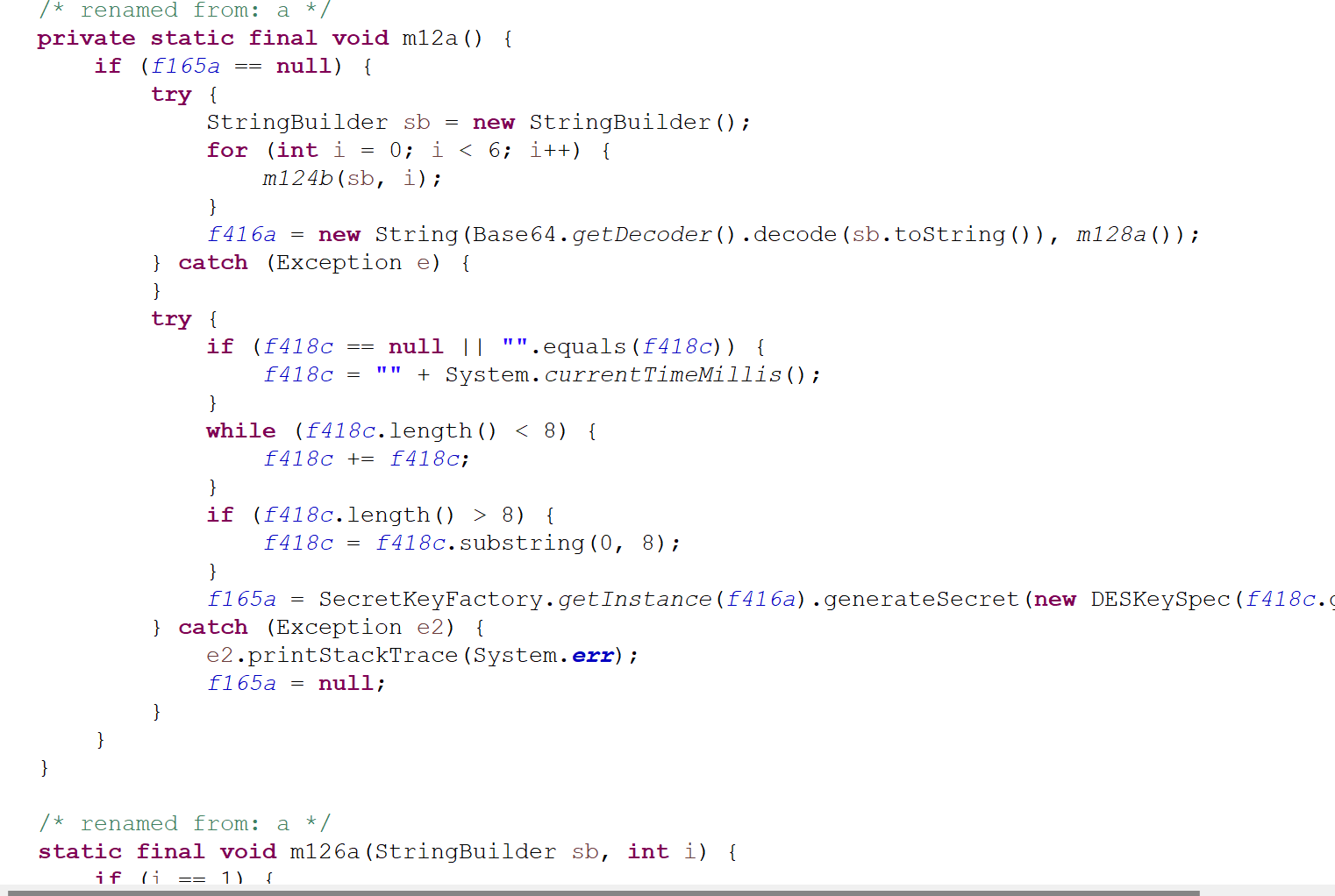
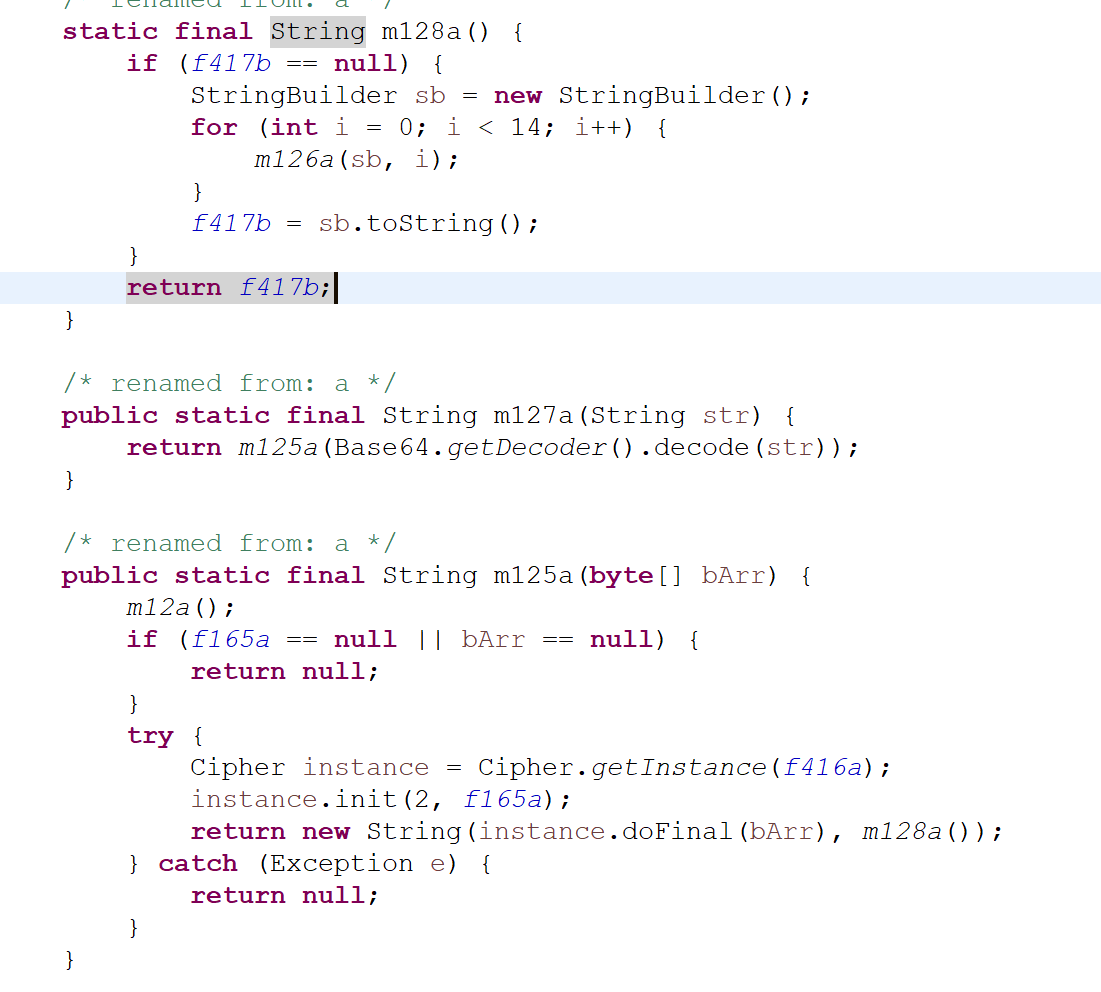
(2) Writeup

[Record how you solve this task here.]

1. 第一题

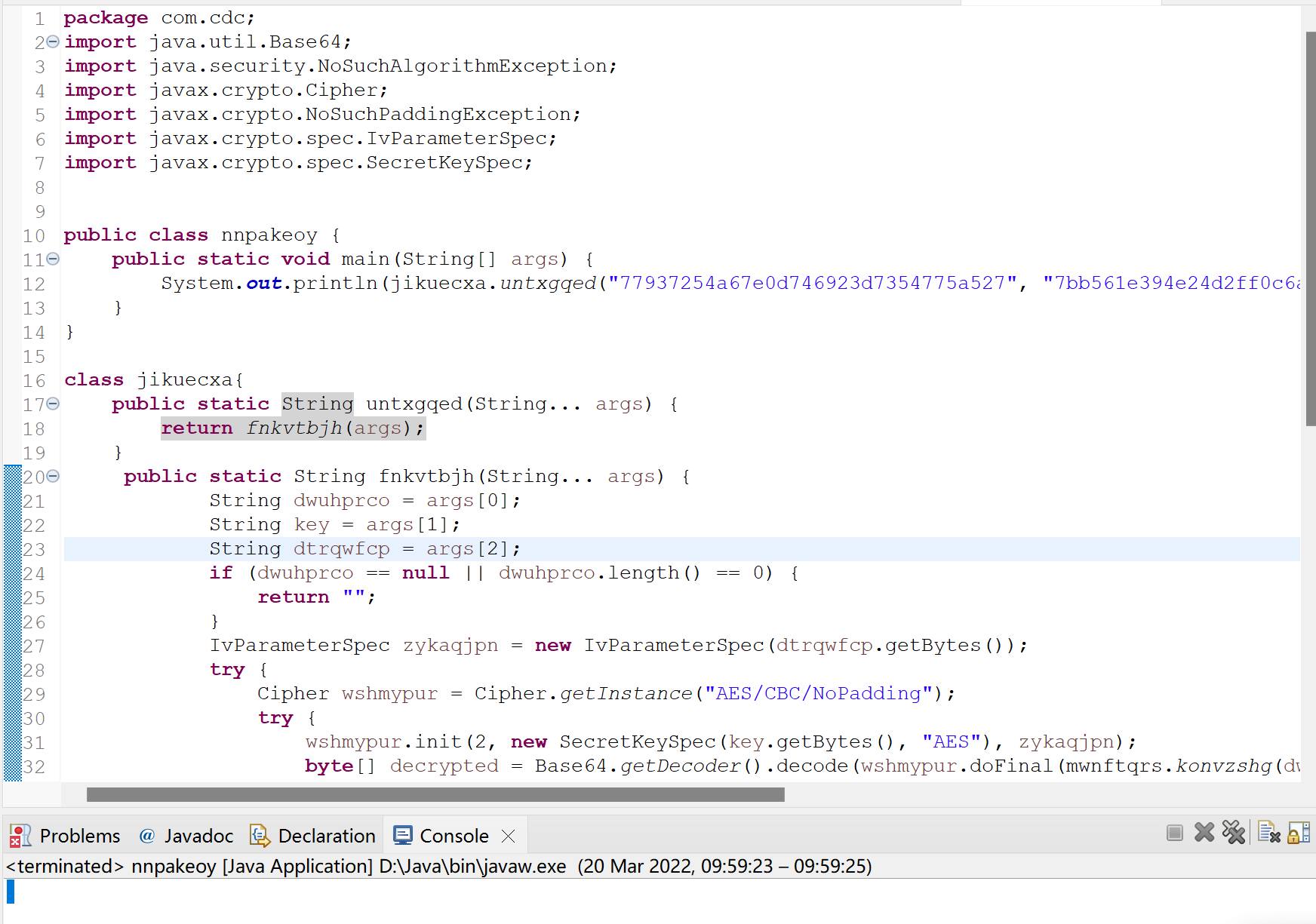


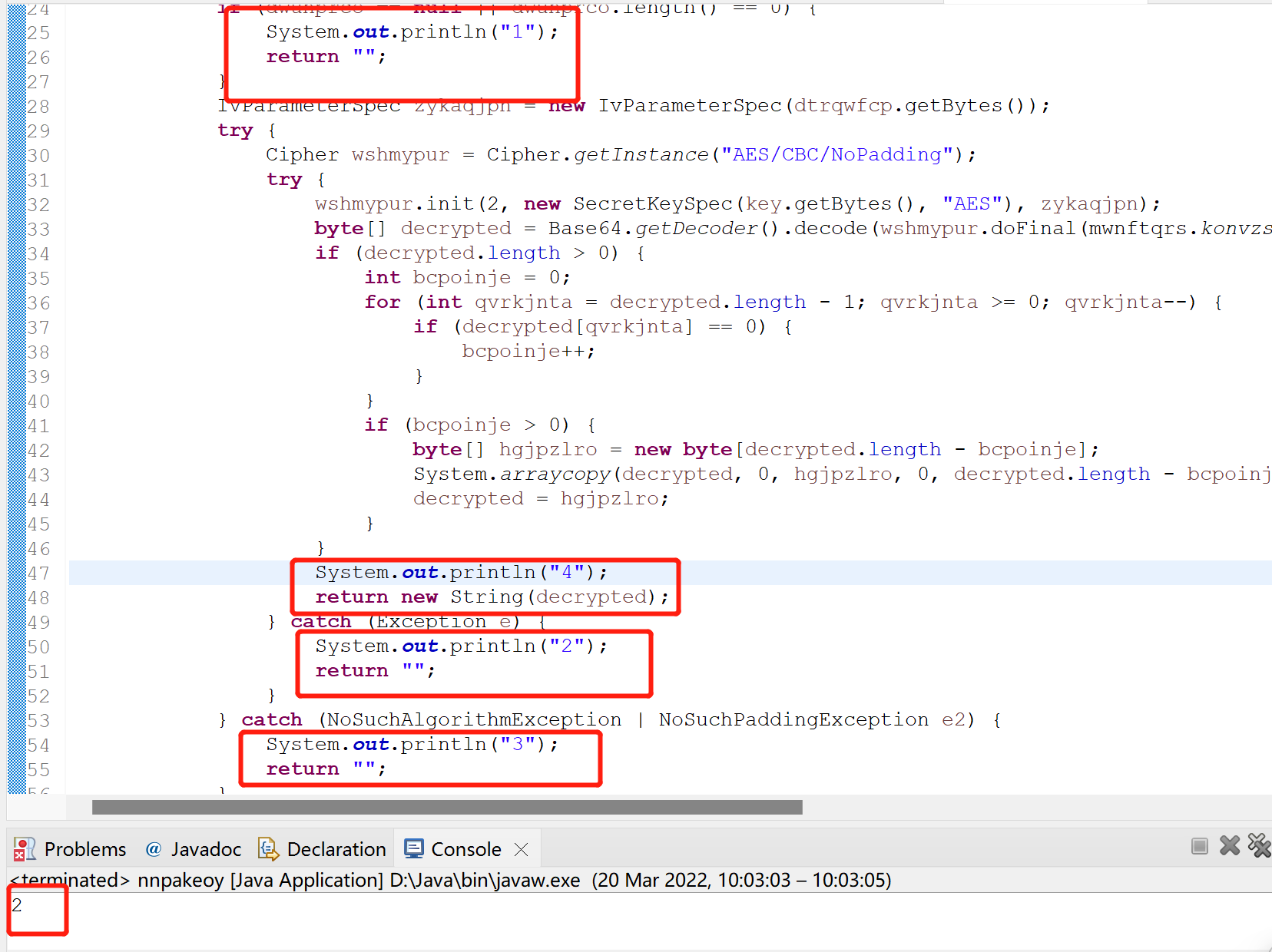
1. 第二题





1. 第三题
   1. 为了验证null，我在代码中填了几行println。（见图2对比）





1. 第四题（部分截图）





