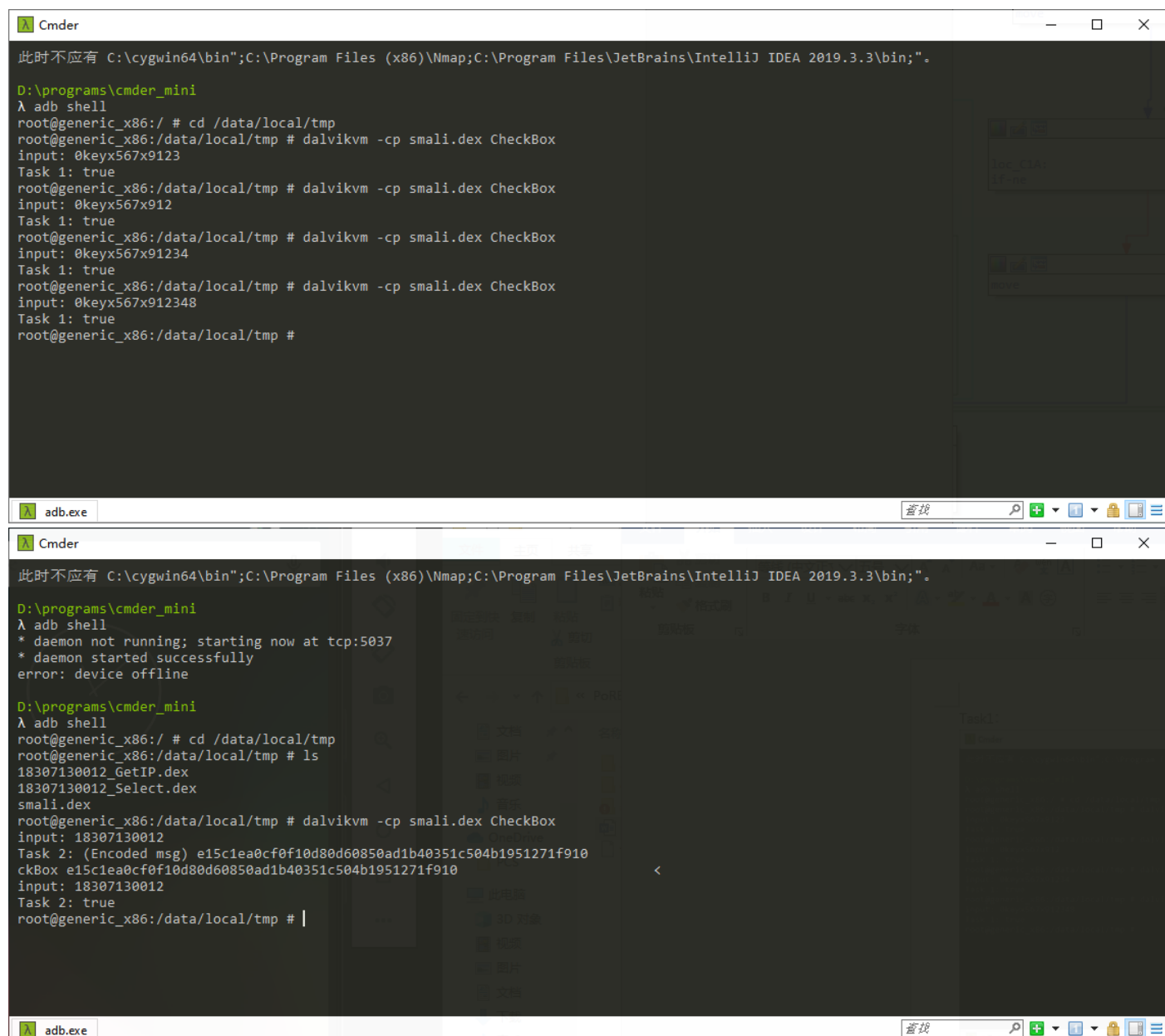


## Smali 代码运行示例:



```
Cmder
此时不应有 C:\cygwin64\bin";C:\Program Files (x86)\Nmap;C:\Program Files\JetBrains\IntelliJ IDEA 2019.3.3\bin;".

D:\programs\cmder_mini
λ adb shell
root@generic_x86:/ # cd /data/local/tmp
root@generic_x86:/data/local/tmp # dalvikvm -cp smali.dex CheckBox
input: 0keyx567x9123
Task 1: true
root@generic_x86:/data/local/tmp # dalvikvm -cp smali.dex CheckBox
input: 0keyx567x912
Task 1: true
root@generic_x86:/data/local/tmp # dalvikvm -cp smali.dex CheckBox
input: 0keyx567x91234
Task 1: true
root@generic_x86:/data/local/tmp # dalvikvm -cp smali.dex CheckBox
input: 0keyx567x912348
Task 1: true
root@generic_x86:/data/local/tmp #

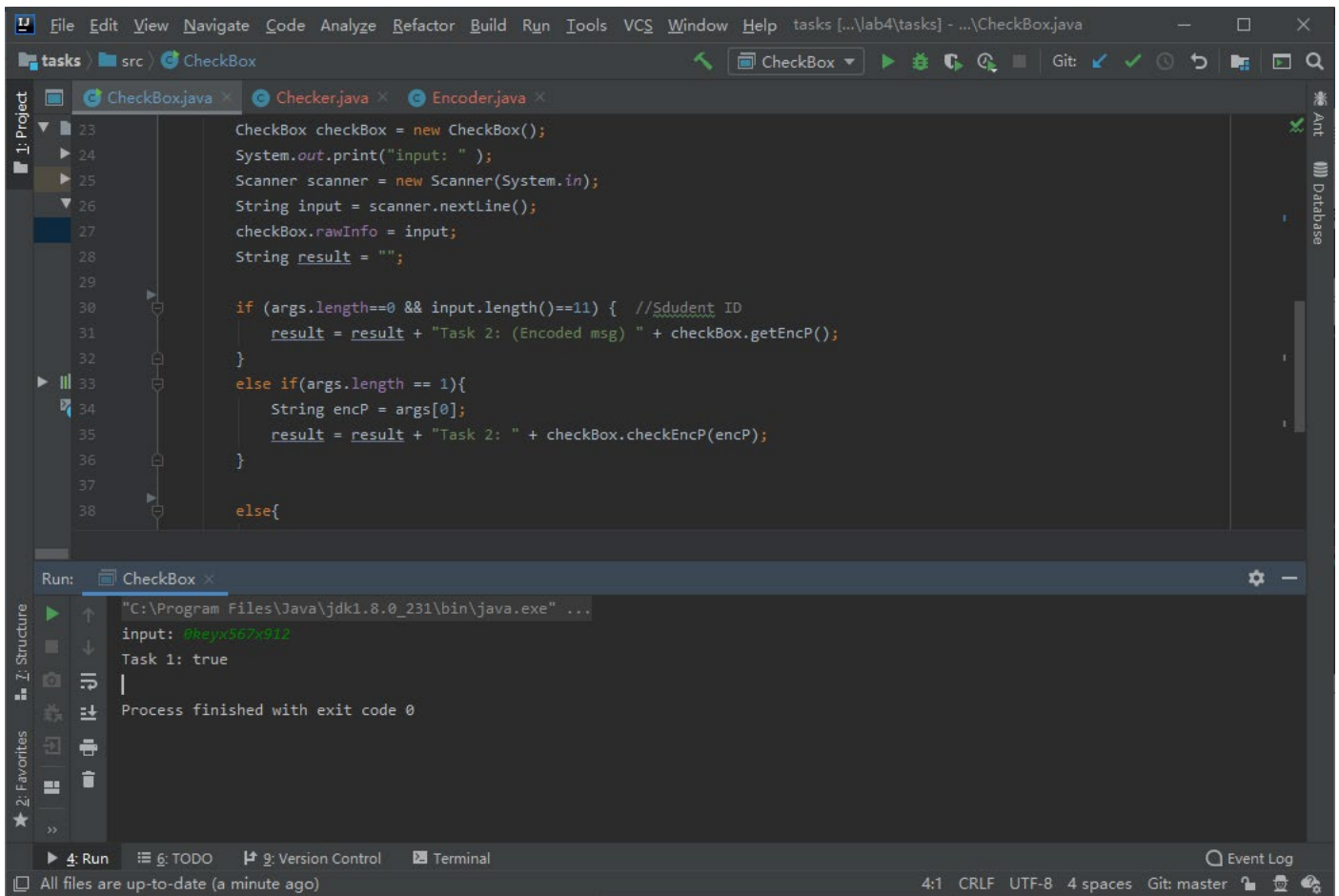
adb.exe

Cmder
此时不应有 C:\cygwin64\bin";C:\Program Files (x86)\Nmap;C:\Program Files\JetBrains\IntelliJ IDEA 2019.3.3\bin;".

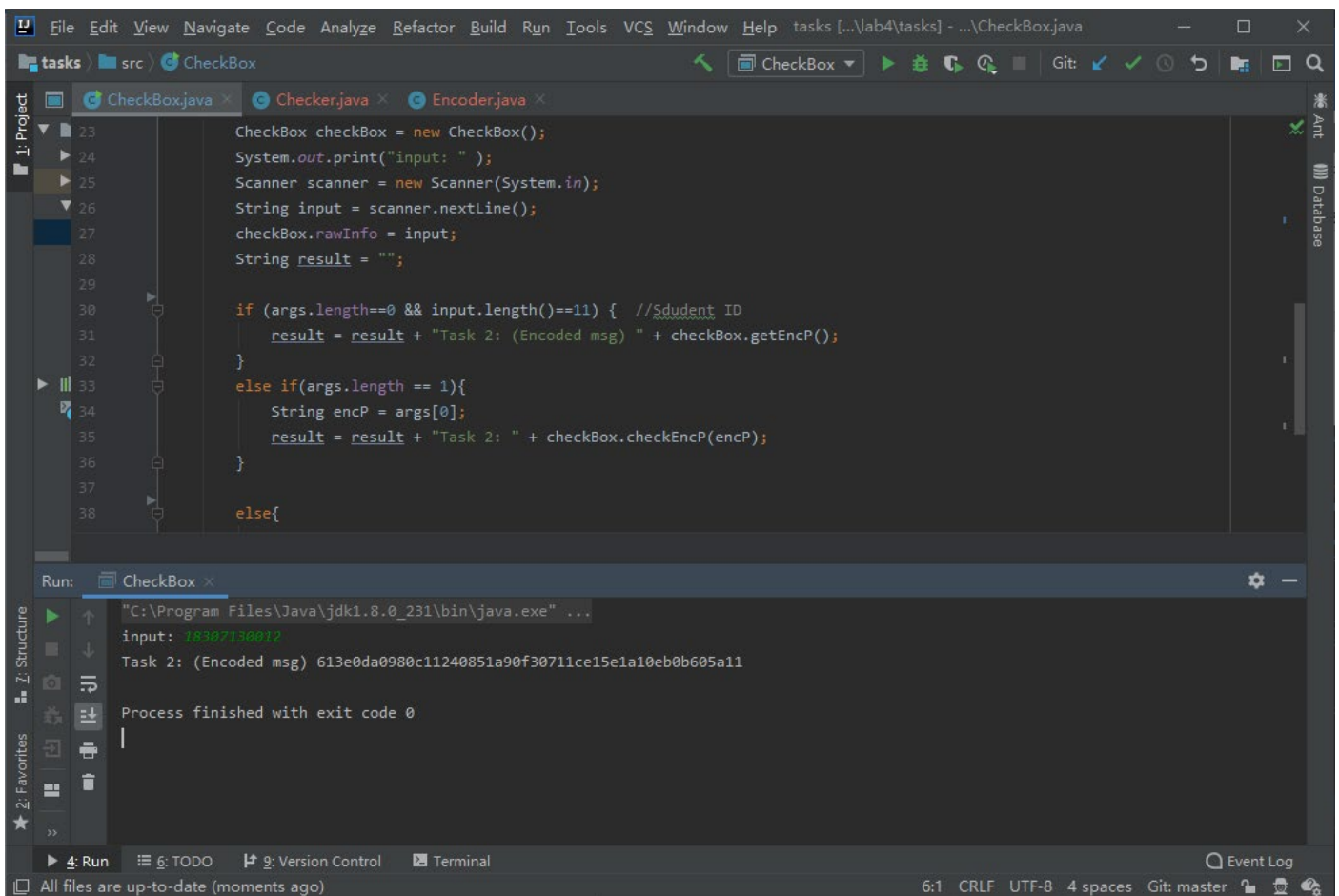
D:\programs\cmder_mini
λ adb shell
* daemon not running; starting now at tcp:5037
* daemon started successfully
error: device offline

D:\programs\cmder_mini
λ adb shell
root@generic_x86:/ # cd /data/local/tmp
root@generic_x86:/data/local/tmp # ls
18307130012_GetIP.dex
18307130012_Select.dex
smali.dex
root@generic_x86:/data/local/tmp # dalvikvm -cp smali.dex CheckBox
input: 18307130012
Task 2: (Encoded msg) e15c1ea0cf0f10d80d60850ad1b40351c504b1951271f910
ckBox e15c1ea0cf0f10d80d60850ad1b40351c504b1951271f910
input: 18307130012
Task 2: true
root@generic_x86:/data/local/tmp #
```

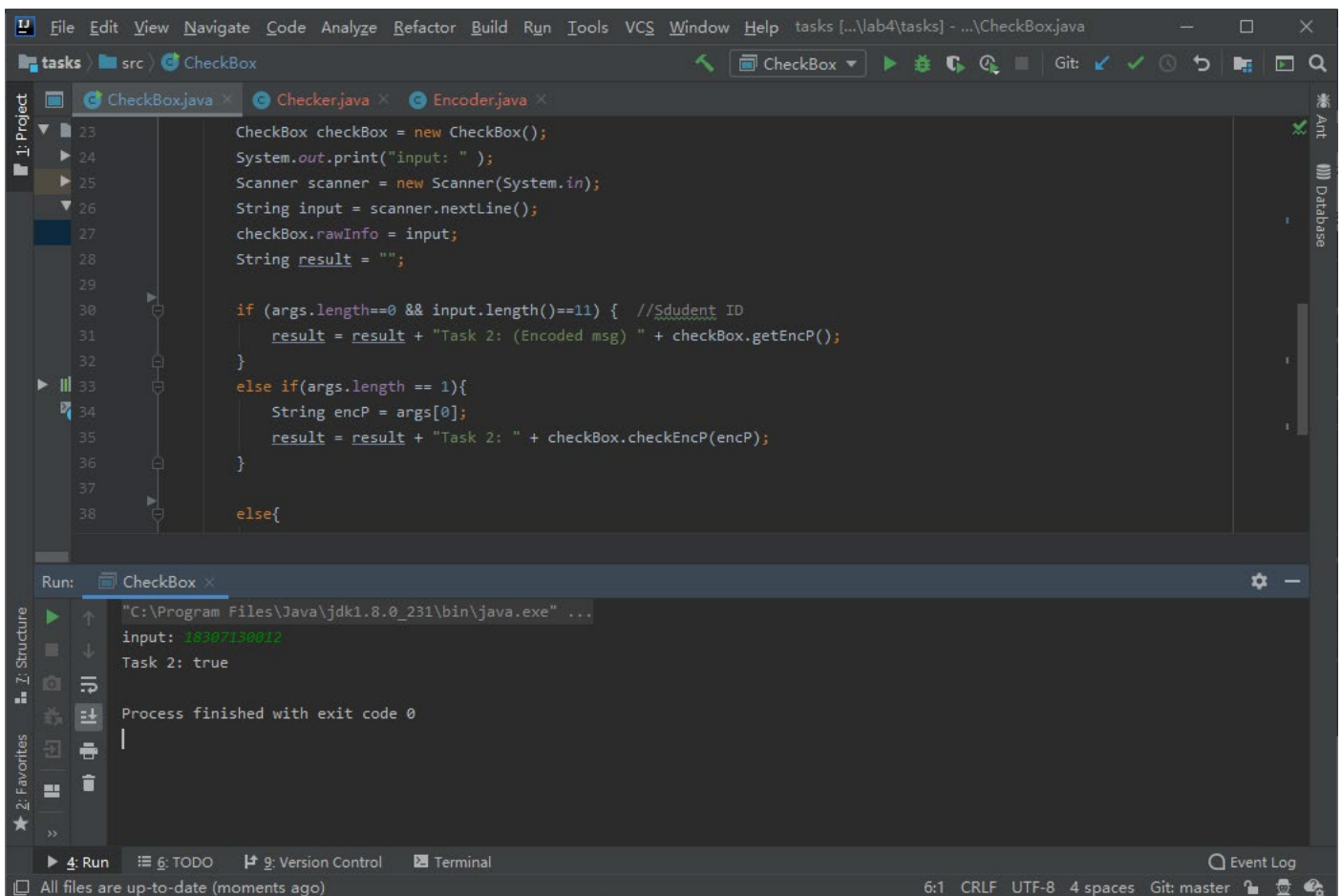
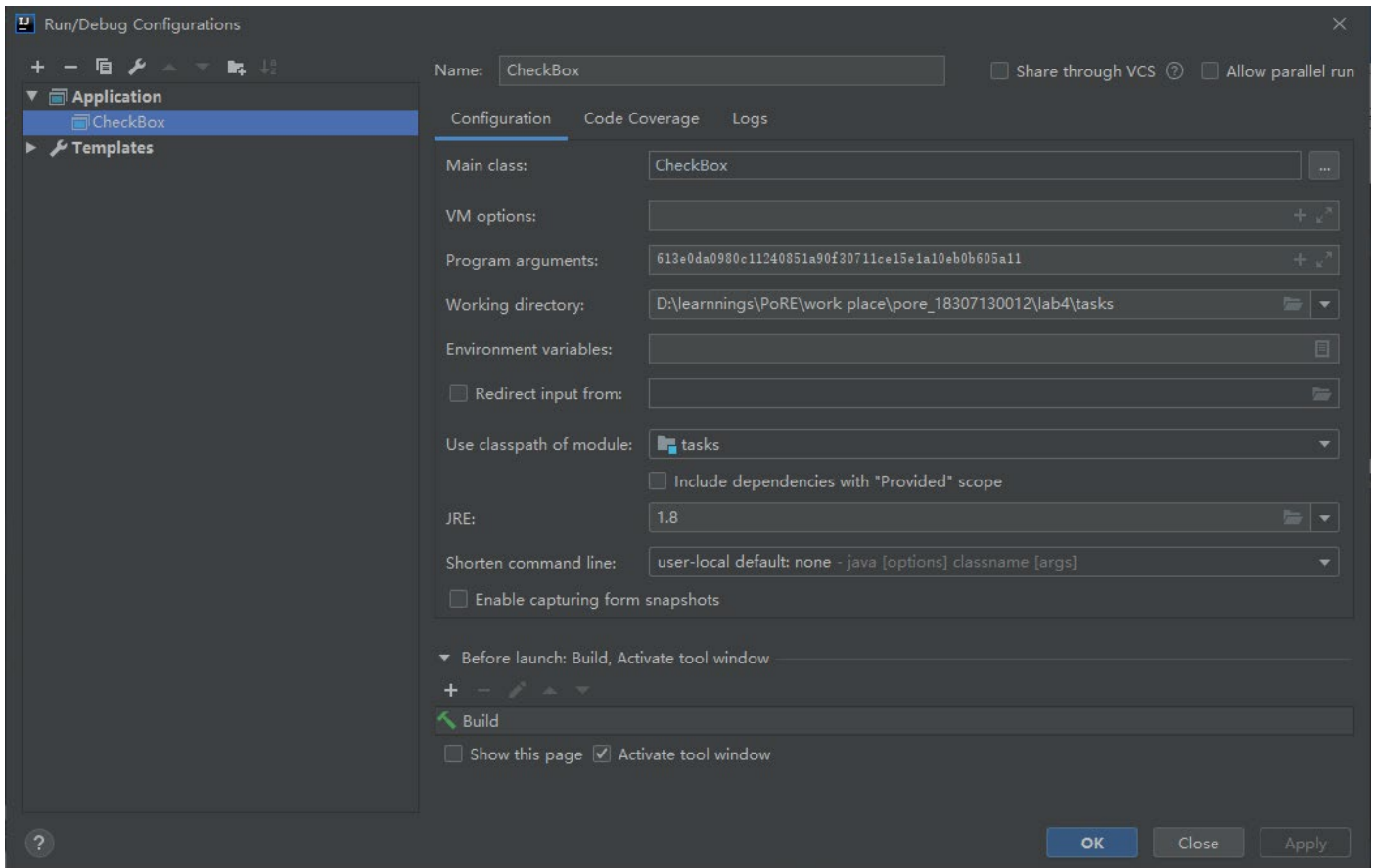
## java 代码运行示例:



```
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help tasks [...\lab4\tasks] - ...\CheckBox.java
tasks src CheckBox
CheckBox.java Checker.java Encoder.java
23 CheckBox checkBox = new CheckBox();
24 System.out.print("input: " );
25 Scanner scanner = new Scanner(System.in);
26 String input = scanner.nextLine();
27 checkBox.rawInfo = input;
28 String result = "";
29
30 if (args.length==0 && input.length()==11) { //Student ID
31     result = result + "Task 2: (Encoded msg) " + checkBox.getEncP();
32 }
33 else if(args.length == 1){
34     String encP = args[0];
35     result = result + "Task 2: " + checkBox.checkEncP(encP);
36 }
37
38 else{
Run: CheckBox x
"C:\Program Files\Java\jdk1.8.0_231\bin\java.exe" ...
input: 0keyx567x912
Task 1: true
Process finished with exit code 0
4: Run 6: TODO 9: Version Control Terminal
All files are up-to-date (a minute ago) 4:1 CRLF UTF-8 4 spaces Git: master
```

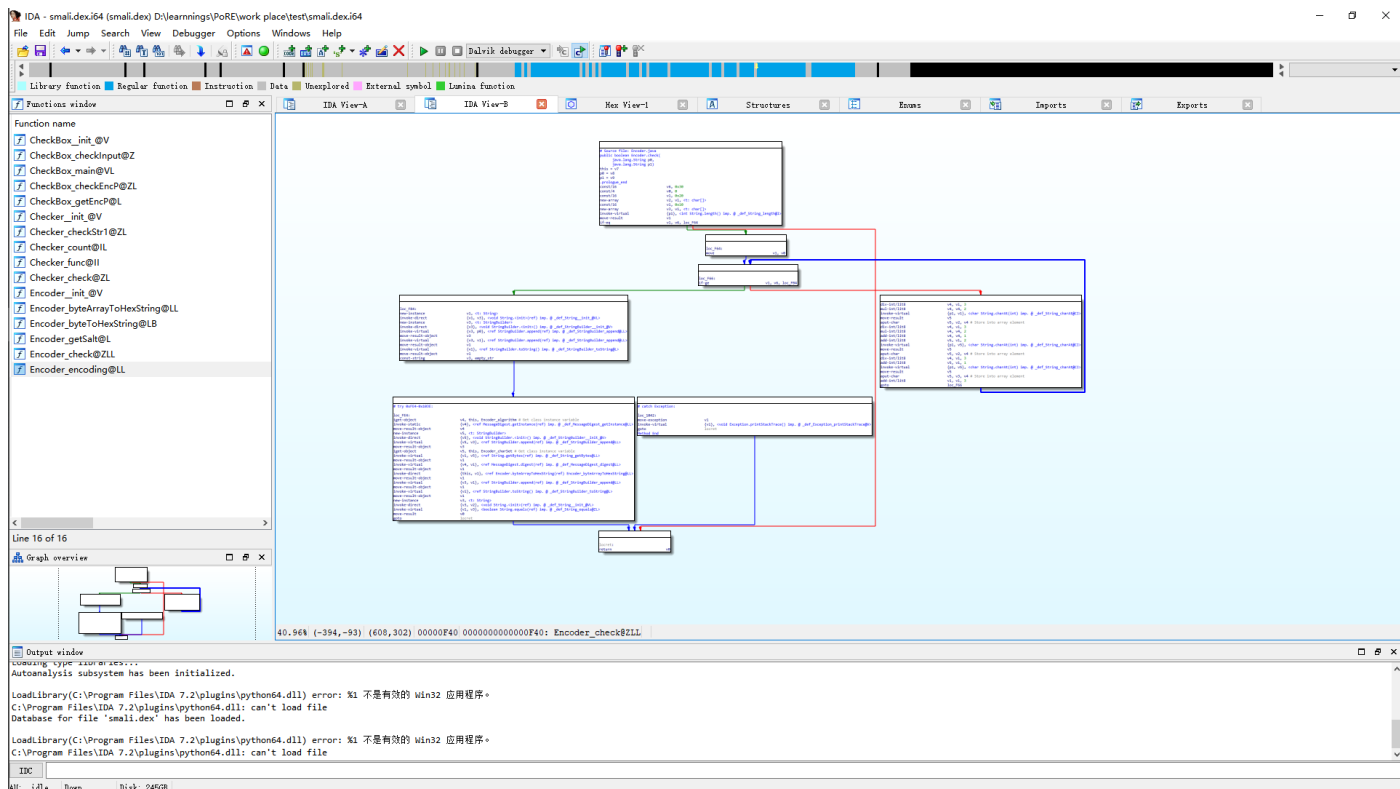


```
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help tasks [...\lab4\tasks] - ...\CheckBox.java
tasks src CheckBox
CheckBox.java Checker.java Encoder.java
23 CheckBox checkBox = new CheckBox();
24 System.out.print("input: " );
25 Scanner scanner = new Scanner(System.in);
26 String input = scanner.nextLine();
27 checkBox.rawInfo = input;
28 String result = "";
29
30 if (args.length==0 && input.length()==11) { //Student ID
31     result = result + "Task 2: (Encoded msg) " + checkBox.getEncP();
32 }
33 else if(args.length == 1){
34     String encP = args[0];
35     result = result + "Task 2: " + checkBox.checkEncP(encP);
36 }
37
38 else{
Run: CheckBox x
"C:\Program Files\Java\jdk1.8.0_231\bin\java.exe" ...
input: 18307130012
Task 2: (Encoded msg) 613e0da0980c11240851a90f30711ce15e1a10eb0b605a11
Process finished with exit code 0
4: Run 6: TODO 9: Version Control Terminal
All files are up-to-date (moments ago) 6:1 CRLF UTF-8 4 spaces Git: master
```

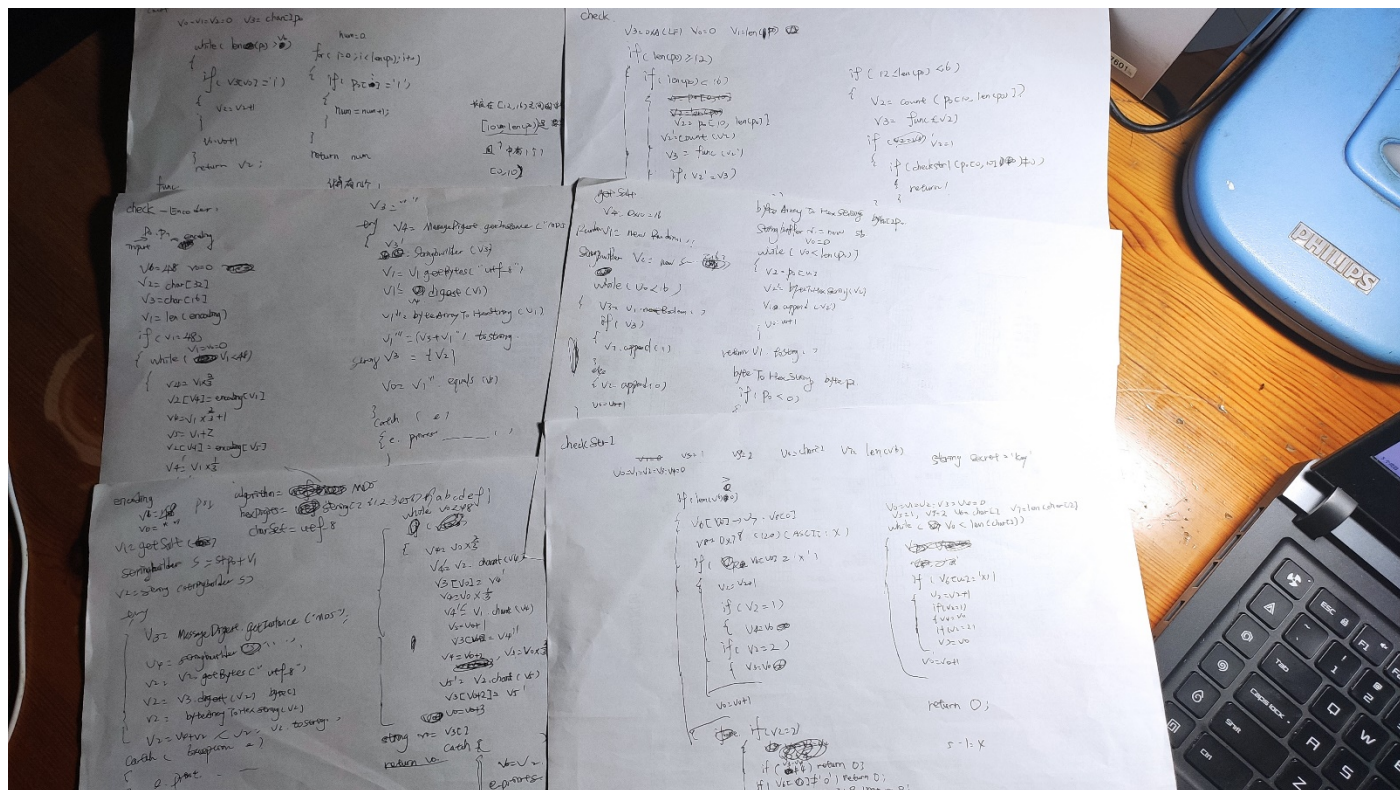


过程:

1、将三个 Smali 文件编译成 dex 文件，使用 IDA Pro 进行处理，形成 CFG。



2、将 Smali 代码粗翻成 java 代码。



3、对于 Task1，推断出程序作用是检测这样一个字符串：

①由字符“0”开头；②字符“0”后接“key”三个字符；③第五个和第九个字符必须是“x”，前十个字符里不



能出现第三个“x”；④第十个字符是“9”；⑤长度为[12,16)个字符；⑥在第十个字符之后的字符里有且只有一个字符“1”。

经过实验，任何符合上述条件的字符串均返回 true，不符合条件的均返回 false。Smali 文件和 java 文件运行结果相同。

4、对于 Task2，推断出程序分为两个部分：加密和验证。

程序中通过随机生成长度为 16 的“0”和“1”构成的字符串作为随机变量。

同时建立了一个将字符数组转换为加密字符串的函数，函数的运行模式是将每个字符的 ascii 码进行哈希映射到“0123456789abcdef”中的两个字符组成的空间中，并将结果拼接成字符串返回。

加密部分将输入字符串和随机字符串拼接后，通过 MD5 进行转换，并使用自建加密函数转换后形成长度为 48 个字符的字符串。再将字符串中每 3 个字符的第一个和第二个存入结果字符串的每 3 个字符的第一和第三个，再将随机字符串的每个字符间隔存入结果字符串每三个字符中的第二个。最后将拼接成的由 48 个字符构成的字符串返回。

验证部分接受两个输入变量：加密字符串和学号。接收输入后，将加密字符串按照每 3 个字符的第一个和第三个存入字符数组 A，第二个存入字符数组 B 的方式，分离随机数串和密码串。再通过与加密部分相同的方式，利用得到的随机数串作为随机数计算加密字符串，如果得出结果和分离出的密码串相同，则返回 true。

通过运行验证，java 程序和 Smali 程序的运行结果相同。

5、通过以上程序和多次运行，确认任务全部完成。