Lab 5. Reversing and Repacking

- ## Task 1

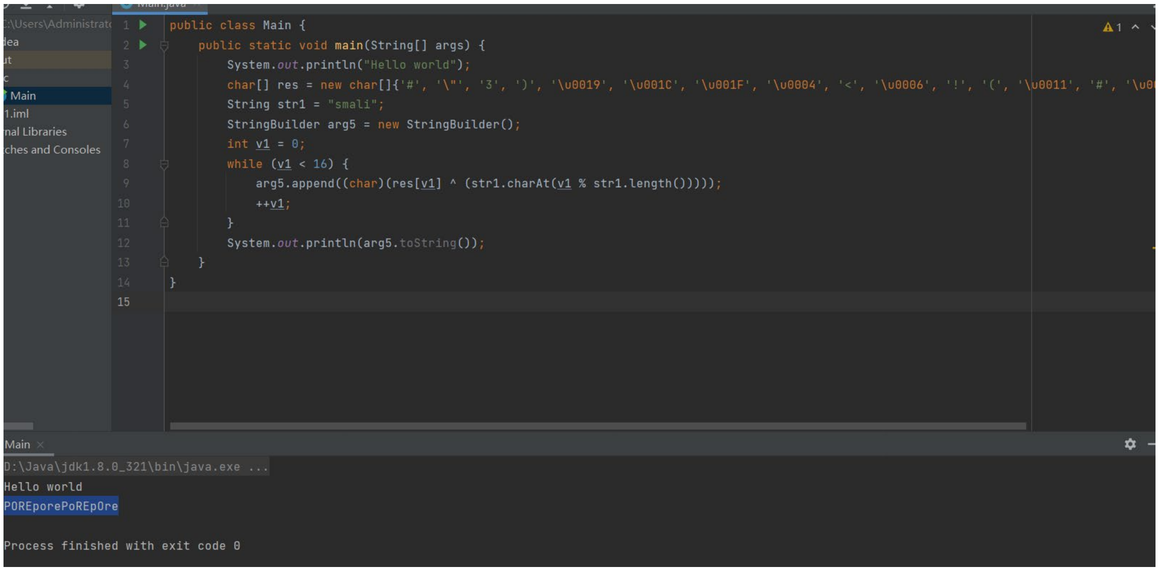
(1) Your Answer

POREporePoREpOre

(2) Writeup

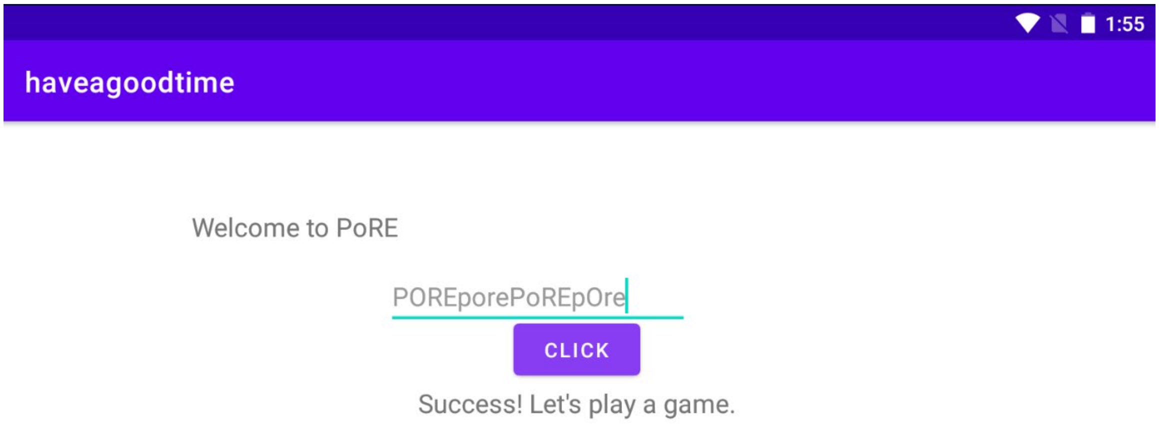
[Record how you solve this task here.]

第一个，简单找到对比的逻辑，写一个逆向程序就行了



```
public class Main {
    public static void main(String[] args) {
        System.out.println("Hello world");
        char[] res = new char[]{'#', '\"', '3', ')', '\u0019', '\u001C', '\u001F', '\u0004', '<', '\u0006', '!', '(', '\u0011', '#', '\u0
        String str1 = "smali";
        StringBuilder arg5 = new StringBuilder();
        int v1 = 0;
        while (v1 < 16) {
            arg5.append((char)(res[v1] ^ (str1.charAt(v1 % str1.length()))));
            ++v1;
        }
        System.out.println(arg5.toString());
    }
}
```

```
D:\Java\jdk1.8.0_321\bin\java.exe ...
Hello world
POREporePoREpOre

Process finished with exit code 0
```



Welcome to PoRE

POREporePoREpOre

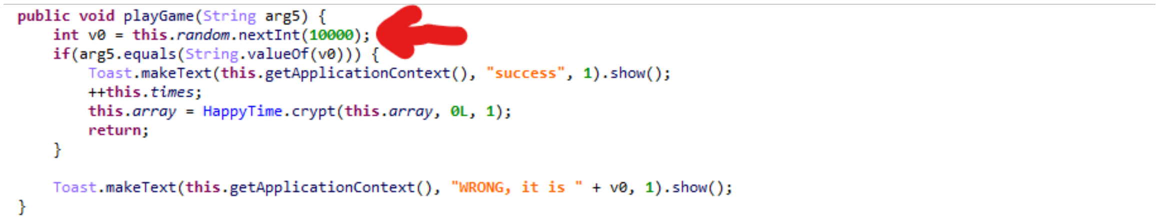
Success! Let's play a game.

- ## Task 2

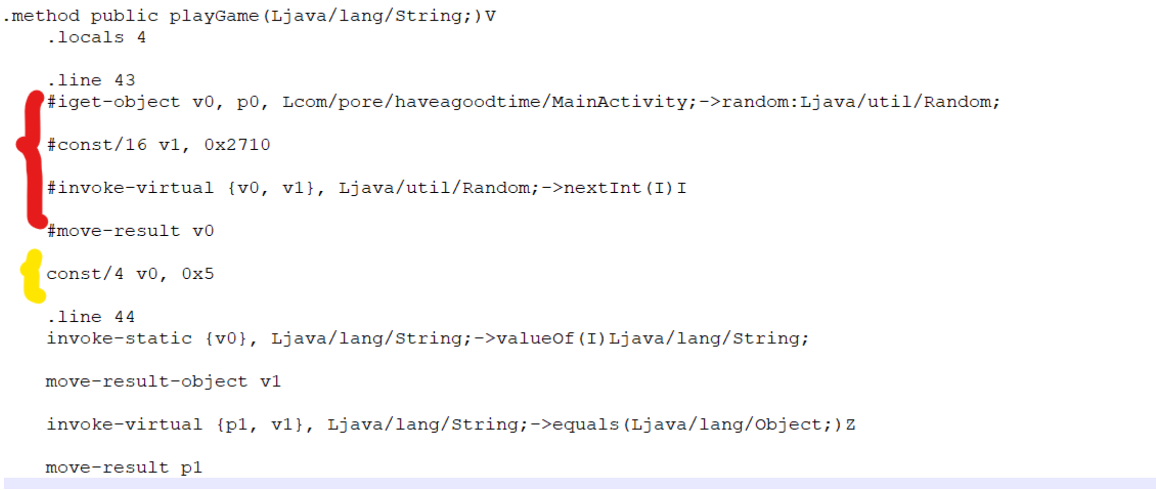
(1) Writeup

[Record how you solve this task here.]

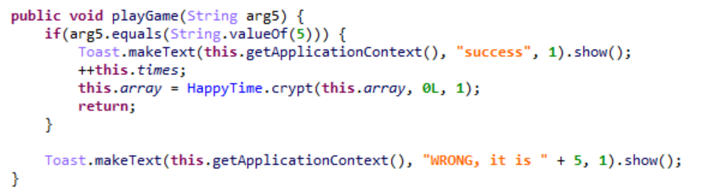
查看代码在 playGame 上的逻辑，发现这一段需要 12 次都与 1-10000 的随机数输入相同，这显然是不能直接做的，不现实，所以就需要用到修改 apk 并重打包的知识了，这里我选择把 random 逻辑直接替换成了使得 v0 变成了一个 int 常量 5。然后连续输 12 次 5 就成功了



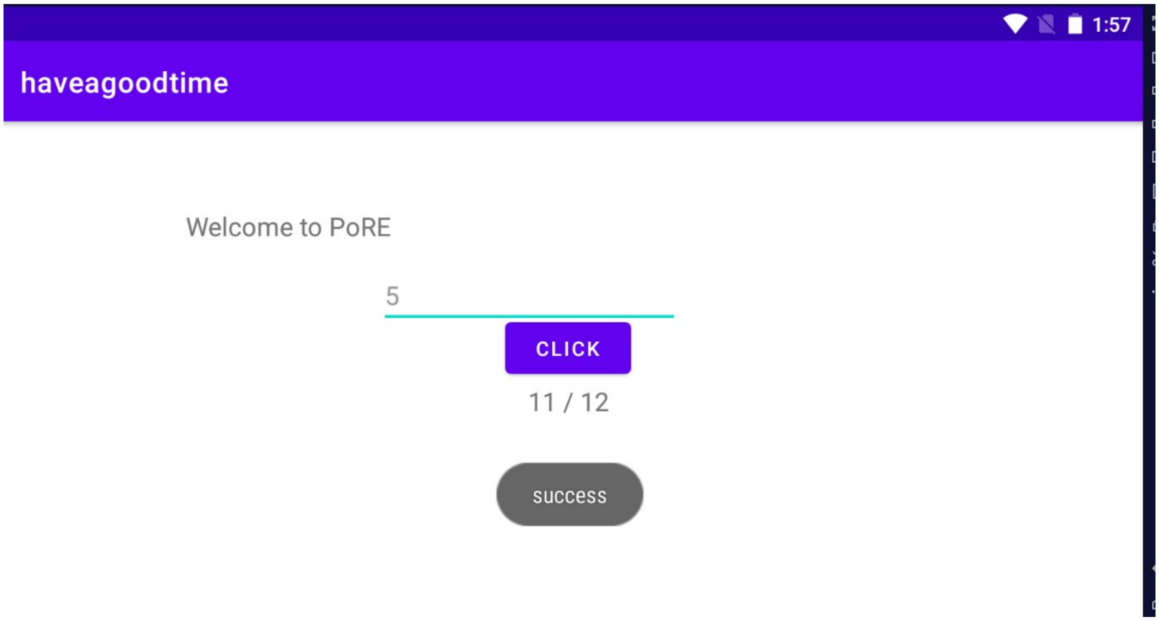
```
public void playGame(String arg5) {
    int v0 = this.random.nextInt(10000);
    if(arg5.equals(String.valueOf(v0))) {
        Toast.makeText(this.getApplicationContext(), "success", 1).show();
        ++this.times;
        this.array = HappyTime.crypt(this.array, 0L, 1);
        return;
    }

    Toast.makeText(this.getApplicationContext(), "WRONG, it is " + v0, 1).show();
}
```



```
.method public playGame(Ljava/lang/String;)V
    .locals 4

    .line 43
    #iget-object v0, p0, Lcom/pore/haveagoodtime/MainActivity;->random:Ljava/util/Random;

    #const/16 v1, 0x2710

    #invoke-virtual {v0, v1}, Ljava/util/Random;->nextInt(I)I

    #move-result v0

    const/4 v0, 0x5

    .line 44
    invoke-static {v0}, Ljava/lang/String;->valueOf(I)Ljava/lang/String;

    move-result-object v1

    invoke-virtual {p1, v1}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result p1
```



```
public void playGame(String arg5) {
    if(arg5.equals(String.valueOf(5))) {
        Toast.makeText(this.getApplicationContext(), "success", 1).show();
        ++this.times;
        this.array = HappyTime.crypt(this.array, 0L, 1);
        return;
    }

    Toast.makeText(this.getApplicationContext(), "WRONG, it is " + 5, 1).show();
}
```



- ## Task3

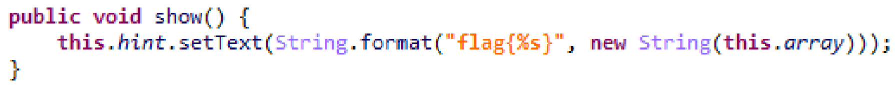
(1) Your Answer

flag{ReversePackage}

(2) Writeup

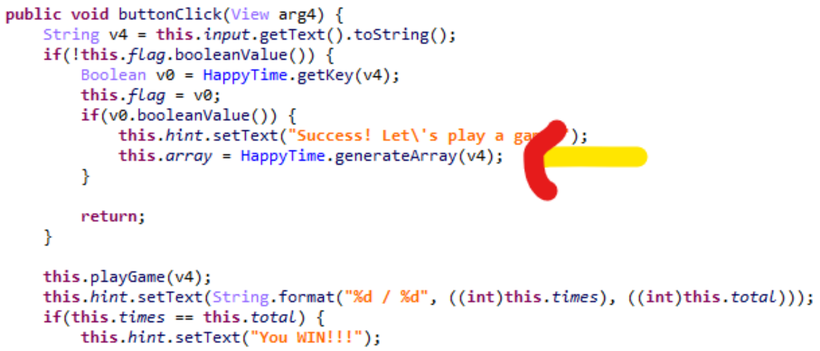
[Record how you solve this task here.]

第三题的逻辑也不难，flag 是在以下函数里进行输出的，但是整个 mainactivity 没有用到这个函数，在 smali 代码中加入就能成



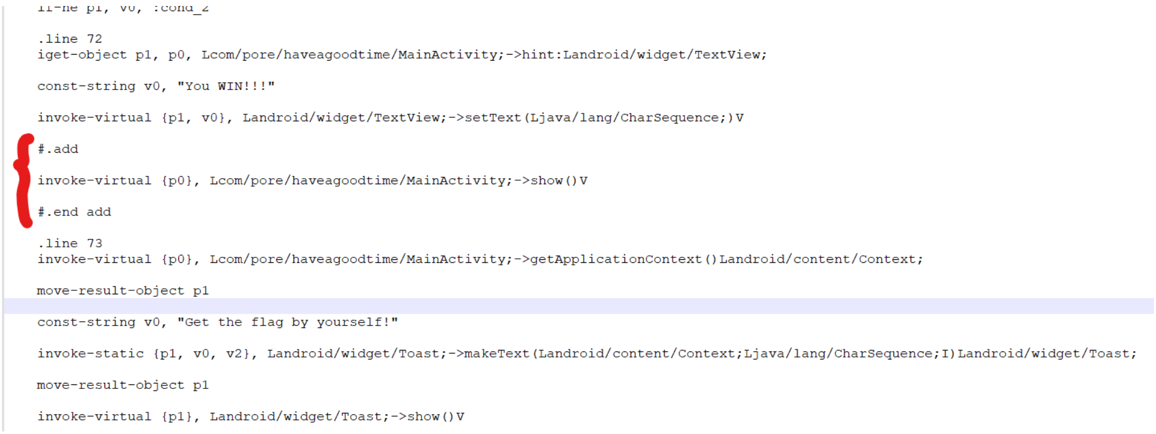
```
public void show() {
    this.hint.setText(String.format("flag{%s}", new String(this.array)));
}
```

当然，加入的位置还有说法，因为一开始的 array 是空的，它在这里被最后确定

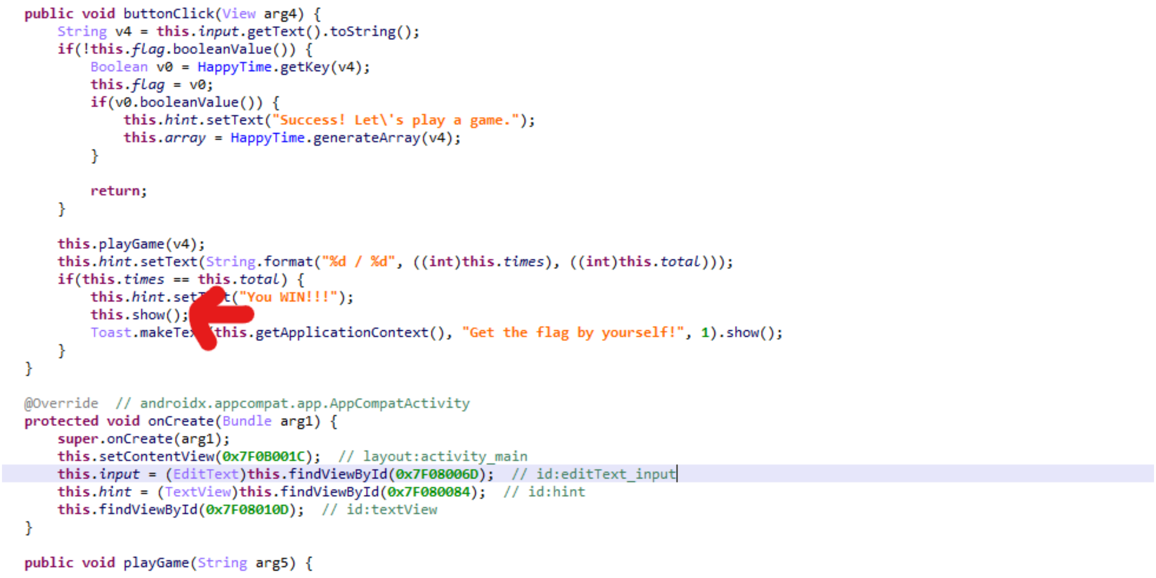


```
public void buttonClick(View arg4) {
    String v4 = this.input.getText().toString();
    if(!this.flag.booleanValue()) {
        Boolean v0 = HappyTime.getKey(v4);
        this.flag = v0;
        if(v0.booleanValue()) {
            this.hint.setText("Success! Let\'s play a ga");
            this.array = HappyTime.generateArray(v4);
        }

        return;
    }

    this.playGame(v4);
    this.hint.setText(String.format("%d / %d", ((int)this.times), ((int)this.total)));
    if(this.times == this.total) {
        this.hint.setText("You WIN!!!");
```

因此，只要在这之后添加一次 show 的函数调用就能拿到 flag，而不需要自己去手写逆向代码了。

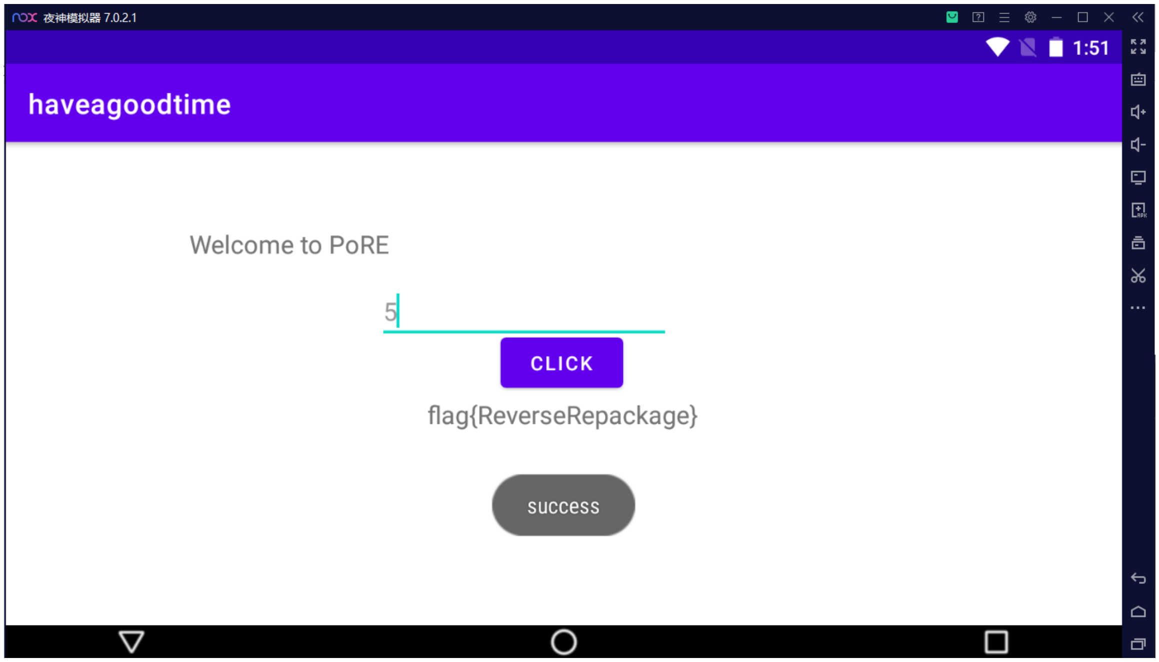


```
    if-ne p1, v0, :cond_2

    .line 72
    iget-object p1, p0, Lcom/pore/haveagoodtime/MainActivity;->hint:Landroid/widget/TextView;

    const-string v0, "You WIN!!!"

    invoke-virtual {p1, v0}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V

    #.add

    invoke-virtual {p0}, Lcom/pore/haveagoodtime/MainActivity;->show()V

    #.end add

    .line 73
    invoke-virtual {p0}, Lcom/pore/haveagoodtime/MainActivity;->getApplicationContext()Landroid/content/Context;

    move-result-object p1

    const-string v0, "Get the flag by yourself!"

    invoke-static {p1, v0, v2}, Landroid/widget/Toast;->makeText(Landroid/content/Context;Ljava/lang/CharSequence;I)Landroid/widget/Toast;

    move-result-object p1

    invoke-virtual {p1}, Landroid/widget/Toast;->show()V
```



```
public void buttonClick(View arg4) {
    String v4 = this.input.getText().toString();
    if(!this.flag.booleanValue()) {
        Boolean v0 = HappyTime.getKey(v4);
        this.flag = v0;
        if(v0.booleanValue()) {
            this.hint.setText("Success! Let\'s play a game.");
            this.array = HappyTime.generateArray(v4);
        }

        return;
    }

    this.playGame(v4);
    this.hint.setText(String.format("%d / %d", ((int)this.times), ((int)this.total)));
    if(this.times == this.total) {
        this.hint.setText("You WIN!!!");
        this.show();
        Toast.makeText(this.getApplicationContext(), "Get the flag by yourself!", 1).show();
    }
}

@Override  // androidx.appcompat.app.AppCompatActivity
protected void onCreate(Bundle arg1) {
    super.onCreate(arg1);
    this.setContentView(0x7F0B001C);  // layout:activity_main
    this.input = (EditText)this.findViewById(0x7F08006D);  // id:editText_input
    this.hint = (TextView)this.findViewById(0x7F080084);  // id:hint
    this.findViewById(0x7F08010D);  // id:textView
}

public void playGame(String arg5) {
```

做完第二 task 任务他就立马把 YOU WIN 覆盖掉出现 flag



Welcome to PoRE

5

flag{ReverseRepackage}

success