**Lab 5. Reversing and Repacking**

* **Task 1**

(1) Your Answer

POREporePoREpOre

(2) Writeup

[Record how you solve this task here.]

通过阅读代码、提取出部分代码，运行得出答案。

public class HelloWorld {

public static void main(String []args) {

int v1=0;

String str1 = "smali";

char[] res;

res = new char[]{'#', '\"', '3', ')', '\u0019', '\u001C', '\u001F', '\u0004', '<', '\u0006', '!', '(', '\u0011', '#', '\u001B', '\u0016'};

while(v1 <16) {

System.out.print((char)(str1.charAt(v1%5)^res[v1]));

++v1;

}

}

}

* **Task 2**

(1) Your Answer

1 1 1 1 1 1 1 1 1 1 1 1

(2) Writeup

我直接修改了随机数的范围，修改为大于等于0小于1，所以一直输入0就行了。

修改后的playGame：

.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, 0x0001

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

move-result v0

.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

const/4 v1, 0x1

if-eqz p1, :cond\_0

.line 45

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

move-result-object p1

const-string v0, "success"

invoke-static {p1, v0, v1}, 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

.line 46

iget p1, p0, Lcom/pore/haveagoodtime/MainActivity;->times:I

add-int/2addr p1, v1

iput p1, p0, Lcom/pore/haveagoodtime/MainActivity;->times:I

.line 47

iget-object p1, p0, Lcom/pore/haveagoodtime/MainActivity;->array:[B

const-wide/16 v2, 0x0

invoke-static {p1, v2, v3, v1}, Lcom/pore/haveagoodtime/HappyTime;->crypt([BJI)[B

move-result-object p1

iput-object p1, p0, Lcom/pore/haveagoodtime/MainActivity;->array:[B

goto :goto\_0

.line 50

:cond\_0

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

move-result-object p1

new-instance v2, Ljava/lang/StringBuilder;

invoke-direct {v2}, Ljava/lang/StringBuilder;-><init>()V

const-string v3, "WRONG, it is "

invoke-virtual {v2, v3}, Ljava/lang/StringBuilder;->append(Ljava/lang/String;)Ljava/lang/StringBuilder;

invoke-virtual {v2, v0}, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;

invoke-virtual {v2}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;

move-result-object v0

invoke-static {p1, v0, v1}, 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

:goto\_0

return-void

.end method

[Record how you solve this task here.]

* **Task 3**

(1) Your Answer

Flag{ReverseRepackage}

(2) Writeup

[Record how you solve this task here.]

我的做法是在完成12次猜数操作后直接调用show函数，由于反编译无法反编译crypt函数，在猜数完成后再去调用show可以避免在猜数过程中flag变化。

修改后的buttonClick：

# virtual methods

.method public buttonClick(Landroid/view/View;)V

.locals 3

.line 57

iget-object p1, p0, Lcom/pore/haveagoodtime/MainActivity;->input:Landroid/widget/EditText;

invoke-virtual {p1}, Landroid/widget/EditText;->getText()Landroid/text/Editable;

move-result-object p1

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

move-result-object p1

.line 58

iget-object v0, p0, Lcom/pore/haveagoodtime/MainActivity;->flag:Ljava/lang/Boolean;

invoke-virtual {v0}, Ljava/lang/Boolean;->booleanValue()Z

move-result v0

if-nez v0, :cond\_1

.line 60

invoke-static {p1}, Lcom/pore/haveagoodtime/HappyTime;->getKey(Ljava/lang/String;)Ljava/lang/Boolean;

move-result-object v0

iput-object v0, p0, Lcom/pore/haveagoodtime/MainActivity;->flag:Ljava/lang/Boolean;

.line 61

invoke-virtual {v0}, Ljava/lang/Boolean;->booleanValue()Z

move-result v0

if-eqz v0, :cond\_0

.line 63

iget-object v0, p0, Lcom/pore/haveagoodtime/MainActivity;->hint:Landroid/widget/TextView;

const-string v1, "Success! Let\'s play a game."

invoke-virtual {v0, v1}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V

.line 64

invoke-static {p1}, Lcom/pore/haveagoodtime/HappyTime;->generateArray(Ljava/lang/String;)[B

move-result-object p1

iput-object p1, p0, Lcom/pore/haveagoodtime/MainActivity;->array:[B

:cond\_0

return-void

.line 68

:cond\_1

invoke-virtual {p0, p1}, Lcom/pore/haveagoodtime/MainActivity;->playGame(Ljava/lang/String;)V

.line 69

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

const/4 v0, 0x2

new-array v0, v0, [Ljava/lang/Object;

const/4 v1, 0x0

iget v2, p0, Lcom/pore/haveagoodtime/MainActivity;->times:I

invoke-static {v2}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;

move-result-object v2

aput-object v2, v0, v1

iget v1, p0, Lcom/pore/haveagoodtime/MainActivity;->total:I

invoke-static {v1}, Ljava/lang/Integer;->valueOf(I)Ljava/lang/Integer;

move-result-object v1

const/4 v2, 0x1

aput-object v1, v0, v2

const-string v1, "%d / %d"

invoke-static {v1, v0}, Ljava/lang/String;->format(Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/String;

move-result-object v0

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

.line 70

iget p1, p0, Lcom/pore/haveagoodtime/MainActivity;->times:I

iget v0, p0, Lcom/pore/haveagoodtime/MainActivity;->total:I

if-ne p1, v0, :cond\_2

.line 72

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

.line 73

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

move-result-object p1

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

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

:cond\_2

return-void

.end method

