WriteUp

100w 这个题就是从 000000-999999 这一百万个密码中找到正确的那一个密码，在经过和黄京帅学长的一系列讨论之后，得出的结论是：貌似只能暴力破解。在综合黄京帅学长和自己在实验吧上看的提示，给出下面两种暴力破解方法（一个一个的试），但仅作参考，不给出结果（因为我也没做）。

一、按键精灵

用按键精灵来进行暴力破解，每分钟大约能尝试 230 个密码左右，100w 个密码的尝试，相应的时间大约是 3 天左右，可以说非常长，而且还不能干其他事。所以可以缩小范围，或者用多台电脑跑。缩小范围是指，有人已经给出正确答案的范围：73000-83000。这个范围已经很小了。按键精灵的代码如下：

```
For 10000
    i = i + 1
    If i < 10 Then
        i = "73000" & i
    End If
    If 9 < i < 100 Then
        i = "7300"&i
    End If
    If 99 < i < 1000 Then
        i="730"&i
    End If
    If 999 < i < 10000 Then
        i="73"&i
    End If
    MoveTo 122, 89
    LeftClick 1
    SayString i
    MoveTo 244, 88
    LeftClick 1
    Hwnd = Plugin.Window.Find(0, "Wrong")
    sWindow = Plugin.Window.IsWindow(Hwnd)
    If sWindow = 1 Then
        MoveTo 579, 313
        LeftClick 1
        MoveTo 122, 89
        LeftClick 1
        KeyPress "Backspace",6
    End If
    Hwnd = Plugin.Window.Find(0, "Right")
    sWindow = Plugin.Window.isWindow(Hwnd)
    If sWindow = 1 Then
        Exit For
    End If
    Next
```

大概都能看懂，语义上没有什么难点，就是操作起来让人很糟心。

二、Java 代码

其实 Java 代码和按键精灵的原理都差不多，都是通过模拟鼠标和按键操作来进行暴力破解。Java 主要是通过 Robot 类的使用，其在 java.awt.*包中，可以自行查阅相关用法。这里，放上黄京帅学长的代码：

```
import java.awt.AWTException;
import java.awt.Color;
import java.awt.Image;
import java.awt.Rectangle;
import java.awt.Robot;
import java.awt.Toolkit;
import java.awt.event.KeyEvent;
import java.awt.image.BufferedImage;
import java.io.File;
import java.io.IOException;

import javax.imageio.ImageIO;

public class test{
    //719,350
    //881,498
    //162,148
    //825,473
    //鼠标 811,472
    //确认 879,474
    public static void main(String args[]){
        try {
            BufferedImage target = null;
            BufferedImage temp = null;
            Robot myRobot = new Robot();
            try {
                target = ImageIO.read(new
File("C:\\Users\\Administrator\\Desktop\\test.png"));
            } catch (IOException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
            }
            myRobot.mouseMove(811, 472);
            myRobot.mousePress(KeyEvent.BUTTON1_DOWN_MASK);
            myRobot.mouseRelease(KeyEvent.BUTTON1_DOWN_MASK);
            for(int i = 0; i < 6; i++){ myRobot.keyPress(KeyEvent.VK_0);
```

```
myRobot.keyRelease(KeyEvent.VK_0);}
            myRobot.mouseMove(879,474);
            myRobot.mousePress(KeyEvent.BUTTON1_DOWN_MASK);
            myRobot.mouseRelease(KeyEvent.BUTTON1_DOWN_MASK);
            temp = myRobot.createScreenCapture(new
Rectangle(Toolkit.getDefaultToolkit().getScreenSize()));
//          int i = 732425;
            int i = 730000;
            int count = 0;
            while(ImageCmp(target, temp)){
                i += 1;count = 0;
                myRobot.delay(50);
                myRobot.mouseMove(825, 473);
                myRobot.mousePress(KeyEvent.BUTTON1_DOWN_MASK);
                myRobot.mouseRelease(KeyEvent.BUTTON1_DOWN_MASK);
                myRobot.mouseMove(811, 472);
                myRobot.mousePress(KeyEvent.BUTTON1_DOWN_MASK);
                myRobot.mouseRelease(KeyEvent.BUTTON1_DOWN_MASK);
                if(i % 10 != 0){
                    myRobot.keyPress(KeyEvent.VK_BACK_SPACE);
                    myRobot.keyRelease(KeyEvent.VK_BACK_SPACE);
                    myRobot.keyPress(KeyEvent.VK_0+(i%10));
                    myRobot.keyRelease(KeyEvent.VK_0+(i%10));
                }else{
                    int k,j;
                    for(k = i; k >= 10; ){
                        if(k % 10 == 0){
                            count ++;
                            k = k / 10;
                        }
                        else break;
                    }
                    k = k % 10;
                    for(j = count; j > 0; j--){
                        myRobot.keyPress(KeyEvent.VK_BACK_SPACE);
                        myRobot.keyRelease(KeyEvent.VK_BACK_SPACE);
                    }
                    myRobot.keyPress(KeyEvent.VK_BACK_SPACE);
                    myRobot.keyRelease(KeyEvent.VK_BACK_SPACE);
                    System.out.println("k="+k);
                    System.out.println("j="+j);
                    myRobot.keyPress(KeyEvent.VK_0+k);
                    myRobot.keyRelease(KeyEvent.VK_0+k);
                    for(j = count; j > 0; j--){
                        myRobot.keyPress(KeyEvent.VK_0);
                        myRobot.keyRelease(KeyEvent.VK_0);
                    }
                }
                System.out.println(i);
                myRobot.mouseMove(879,474);
                myRobot.mousePress(KeyEvent.BUTTON1_DOWN_MASK);
                myRobot.mouseRelease(KeyEvent.BUTTON1_DOWN_MASK);
                myRobot.delay(200);
                temp                =                myRobot.createScreenCapture(new
Rectangle(Toolkit.getDefaultToolkit().getScreenSize()));
            }
            File f = new File("C:\\Users\\Administrator\\Desktop\\temp.png");
            try {
                ImageIO.write(temp, "png", f);
            } catch (IOException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
            }
            return;
        } catch (AWTException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
    }
    private static boolean ImageCmp(BufferedImage I1, BufferedImage I2){
        int i = 723;
        int j = 359;
        Color tmp1;
        Color tmp2;
        for(i = 723; i <= 768; i++){
            for(j = 359; j <= 372; j++){
                tmp1 = new Color(I1.getRGB(i, j));
                tmp2 = new Color(I2.getRGB(i, j));
                if(ColorCmp(tmp1,tmp2));
                else return false;
            }
        }if(i > 768 && j > 372)
            return true;
        else return false;
    }
    private static boolean ColorCmp(Color C1,Color C2){
        if(-10 <= C1.getRed() - C2.getRed() && C1.getRed() - C2.getRed() <= 10){
            if(-10 <= C1.getBlue() - C2.getBlue() && C1.getBlue() - C2.getBlue() <= 10){
                if(-10 <= C1.getGreen() - C2.getGreen() && C1.getGreen() - C2.getGreen() <= 10)
                    return true;
                else return false;
            }else return false;
        }else return false;
    }
}
```

可以拿去跑一下~

非常感谢黄京帅学长提供的代码和建议，这道题感觉太简单粗暴了，暂时还没想出其他方法来解决这个问题。先将就看吧~