1. Change .apk to .zip, unzip new zip file and cd into unzipped file

```
┌──(kali㉿kali-vm)-[~/Desktop/SHC/ctf_bundle_1_3/crackme-apk]
└─$ ls
apk-decode  crackme-apk  CrackMeSimple.apk  CrackMeUnZip  CrackMeZip.zip  decipher.java  jd-gui

┌──(kali㉿kali-vm)-[~/Desktop/SHC/ctf_bundle_1_3/crackme-apk]
└─$ cd CrackMeUnZip

┌──(kali㉿kali-vm)-[~/…/SHC/ctf_bundle_1_3/crackme-apk/CrackMeUnZip]
└─$
```

2. Use dex2jar (https://github.com/pxb1988/dex2jar) to convert classes.dex to a jar file ("old_classes.dex -> new_classes.jar" in my example)
   Although there is an error message, the java code is still readable.

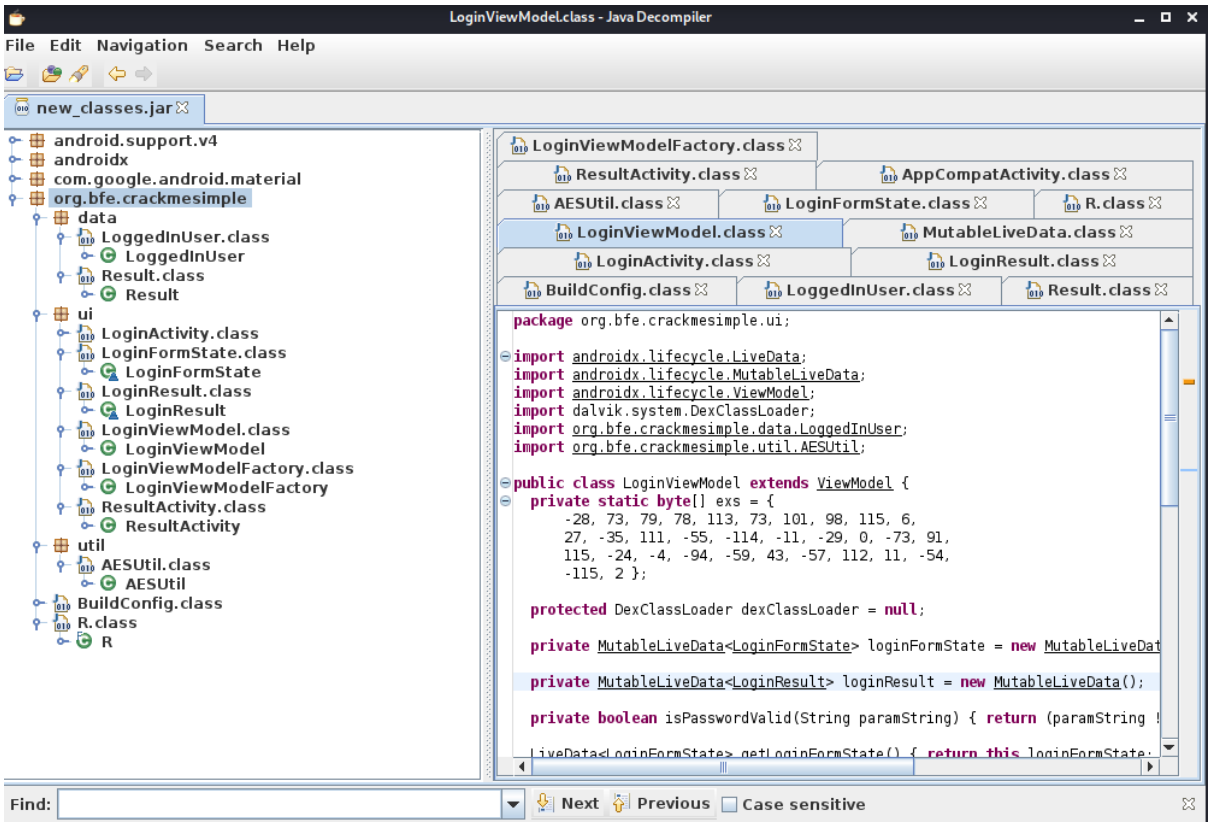
```
┌──(kali㉿kali-vm)-[~/…/SHC/ctf_bundle_1_3/crackme-apk/CrackMeUnZip]
└─$ l
AndroidManifest.xml*  META-INF/  new_classes.jar  old_classes.dex*  old_classes-error.zip  res/  resources.arsc*

┌──(kali㉿kali-vm)-[~/…/SHC/ctf_bundle_1_3/crackme-apk/CrackMeUnZip]
└─$ sh /opt/dex2jar/d2j-dex2jar.sh old_classes.dex
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
dex2jar old_classes.dex → ./old_classes-dex2jar.jar
Detail Error Information in File ./old_classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

┌──(kali㉿kali-vm)-[~/…/SHC/ctf_bundle_1_3/crackme-apk/CrackMeUnZip]
└─$ ls
AndroidManifest.xml  new_classes.jar  old_classes-dex2jar.jar  res
META-INF             old_classes.dex  old_classes-error.zip    resources.arsc

┌──(kali㉿kali-vm)-[~/…/SHC/ctf_bundle_1_3/crackme-apk/CrackMeUnZip]
└─$
```

3. Open the new_classes.jar in jd-gui (https://github.com/java-decompiler/jd-gui) and locate the LoginViewModel & AESUtil Class.



4. Copy the encrypted flag (as the byte array “exs”) and the decrypt, makeKey & makeIV methods in the AESUtil class.

```java
public class Main {
    private static final String ENCRYPTION_IV = "SHCUOkfd89ut7777";

    private static final String ENCRYPTION_KEY = "Simpleji4todnkfL";

    public static byte[] exs = {
        -28, 73, 79, 78, 113, 73, 101, 98, 115, 6,
        27, -35, 111, -55, -114, -11, -29, 0, -73, 91,
        115, -24, -4, -94, -59, 43, -57, 112, 11, -54,
        -115, 2 };

    public static String str = new String(decrypt(exs));

    public static void main (String[] args) {
        System.out.println("Flag: " + str);
    }

    public static byte[] decrypt(byte[] paramArrayOfByte) {
        try {
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
            cipher.init(2, makeKey(), makeIv());
            //cipher.init(2, "Simpleji4todnkfL", "SHCUOkfd89ut7777");
            return cipher.doFinal(paramArrayOfByte);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

    static AlgorithmParameterSpec makeIv() {
        try {
            return new IvParameterSpec("SHCUOkfd89ut7777".getBytes("UTF-8"));
        } catch (UnsupportedEncodingException unsupportedEncodingException) {
            unsupportedEncodingException.printStackTrace();
            return null;
        }
    }

    static Key makeKey() {
        try {
            return new SecretKeySpec(MessageDigest.getInstance("SHA-256").digest("Simpleji4todnkfL".getBytes("UTF-8")), "AES");
        } catch (NoSuchAlgorithmException noSuchAlgorithmException) {
            noSuchAlgorithmException.printStackTrace();
        } catch (UnsupportedEncodingException unsupportedEncodingException) {
            unsupportedEncodingException.printStackTrace();
        }
            return null;
    }
}
```

The Imports did not fit into the screenshot, but they are identical to the imports in the AESUtil class.

5. Run the java programm

```
┌──(kali㉿kali-vm)-[~/Desktop/SHC/ctf_bundle_1_3/crackme-apk]
└─$ java decipher.java
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Flag: HL{R3v3rsing.FUN}

┌──(kali㉿kali-vm)-[~/Desktop/SHC/ctf_bundle_1_3/crackme-apk]
└─$
```