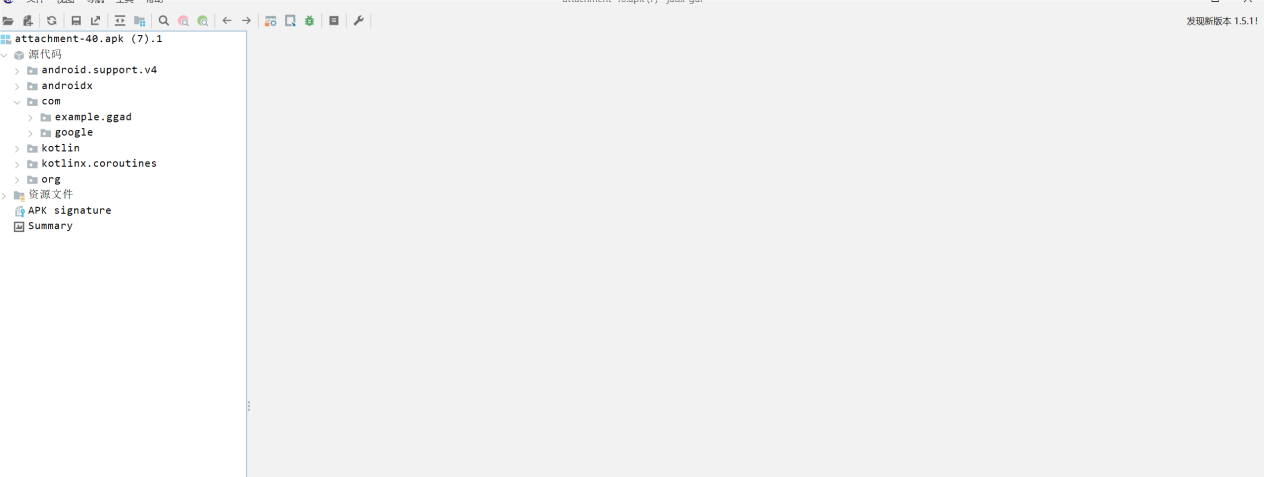
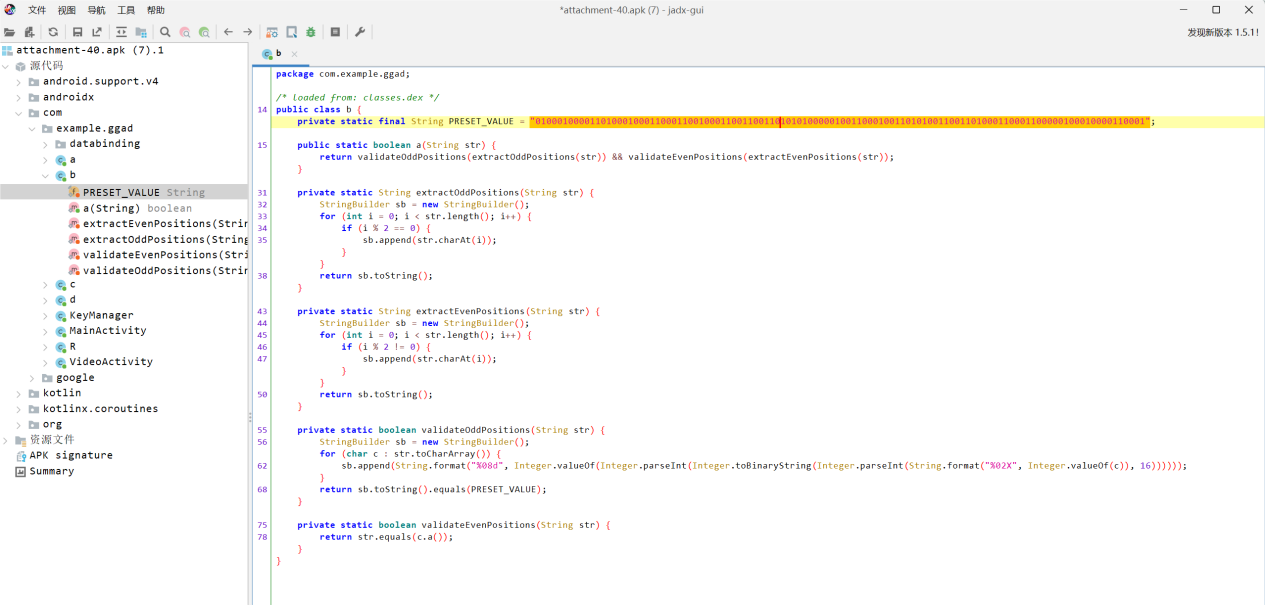
# Mobile1

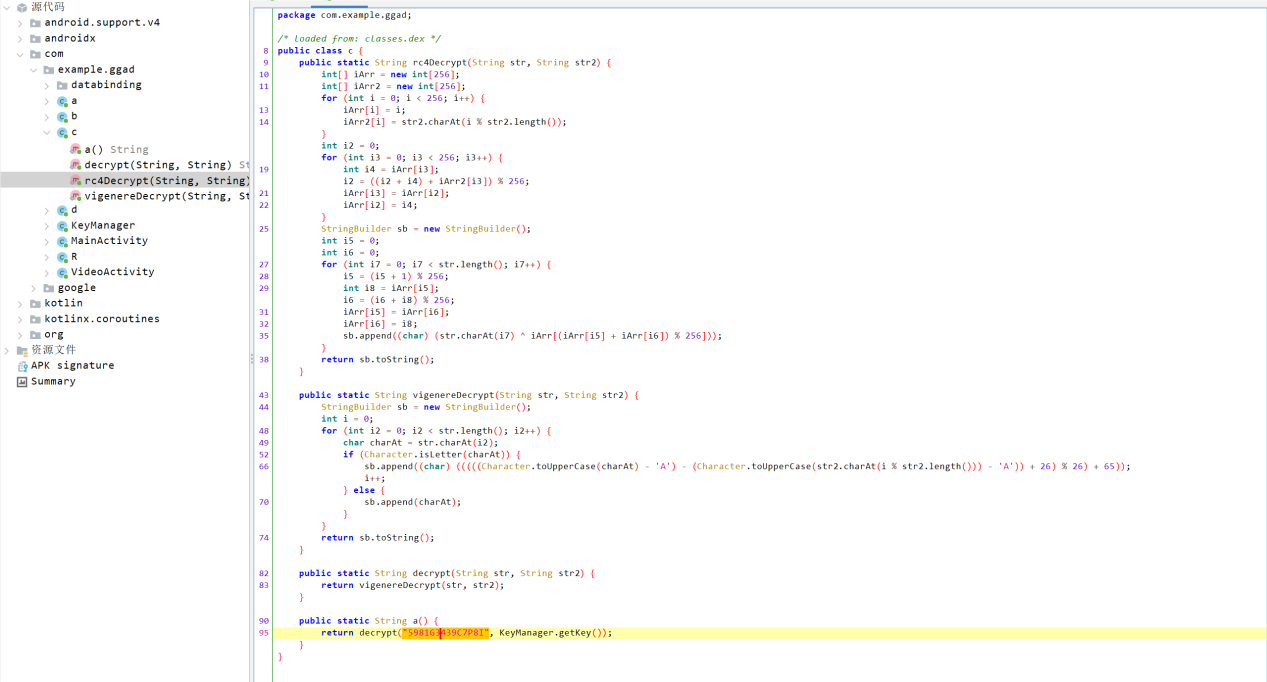
用jadx打开下载的apk文件



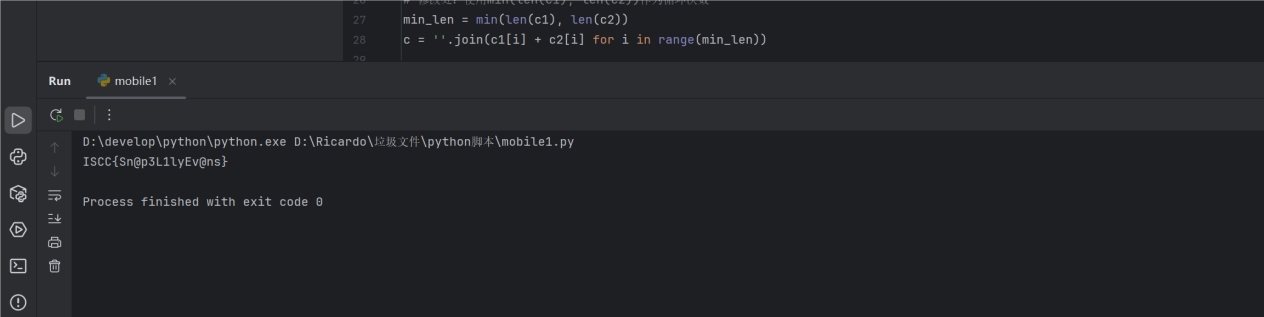
Com->example.ggad->b->preset\_value找到以下数据



Com->example.ggad->c找到以下数据



将这两串数据替换到脚本,跑出flag



Exp:

ci = '0100010000110100010001100011001000110011001101010100000100110001001101010011001101000110001100000100010000110001'

c0 = '5981G3439C7P8I'

def vigenere\_decrypt(text, key):

decrypted = []

key\_shifts = [ord(k.upper()) - ord('A') for k in key]

key\_len, key\_idx = len(key\_shifts), 0

for char in text:

if char.isalpha():

shift = key\_shifts[key\_idx % key\_len]

upper\_char = char.upper()

decrypted\_code = (ord(upper\_char) - ord('A') - shift) % 26 + ord('A')

decrypted\_char = chr(decrypted\_code)

decrypted.append(decrypted\_char.lower() if char.islower() else decrypted\_char)

key\_idx += 1

else:

decrypted.append(char)

return ''.join(decrypted)

def a(cs):

return vigenere\_decrypt(cs, 'ExpectoPatronum')

c2 = a(c0)

c1 = ''.join(chr(int(ci[i:i+8], 2)) for i in range(0, len(ci), 8))

# 修改处：使用min(len(c1), len(c2))作为循环次数

min\_len = min(len(c1), len(c2))

c = ''.join(c1[i] + c2[i] for i in range(min\_len))

byte\_array = [int(c[i:i+2], 16) for i in range(0, len(c), 2)]

c3 = ''.join(f"{b:08b}" for b in byte\_array)

str1 = c3.translate(str.maketrans('01', '10'))

c4 = bytes(int(str1[i:i+8], 2) for i in range(0, len(str1), 8))

def rc4\_ksa(key):

key = key.encode() if isinstance(key, str) else key

S = list(range(256))

j = 0

for i in range(256):

j = (j + S[i] + key[i % len(key)]) % 256

S[i], S[j] = S[j], S[i]

return S

def rc4\_prga(S, data):

data = data if isinstance(data, bytes) else data.encode()

i = j = 0

result = []

for byte in data:

i = (i + 1) % 256

j = (j + S[i]) % 256

S[i], S[j] = S[j], S[i]

result.append(byte ^ S[(S[i] + S[j]) % 256])

return bytes(result)

S = rc4\_ksa('ExpectoPatronum')

res = rc4\_prga(S, c4)

flag = f"ISCC{{{res.decode()}}}"

print(flag)