Week 1

Re

easyasm

把文件拖进IDA里面看汇编，大概用C语言表达一下加密过程，然后根据加密逆向解密

```c
#include<stdio.h>
int main(void)
{
    char s[] = "hgame{Fill_in_your_flag}";
    int e[] = { 0x91, 0x61, 0x01, 0xC1, 0x41, 0xA0, 0x60, 0x41, 0xD1, 0x21,0x14, 0xC1, 0x41, 0xE2, 0x50, 0xE1, 0xE2, 0x54, 0x20, 0xC1,0xE2, 0x60, 0x14, 0x30, 0xD1, 0x51, 0xC0,
    for (int i = 0; i < 28; i++)//逆向解密
    {
        e[i] ^= 23;
        e[i] = (e[i]>>4)+(e[i]<<4);
    }
    for (int i = 0; i < 28; i++)
    {
        printf("%c", e[i]);
    }
    /*for (int i = 0; s[i] != '\0'; )  //加密过程
    {
        s[i]=((s[i]<<4)+(s[i]>>4))^23;
        i++;
        if (s[i] - e[i - 1] != 0)
        {
            printf("wrong\n");
            break;
        }
        else if (i == 28)
        {
            printf("right\n");
            break;
        }
        else
            continue;
```

creakme

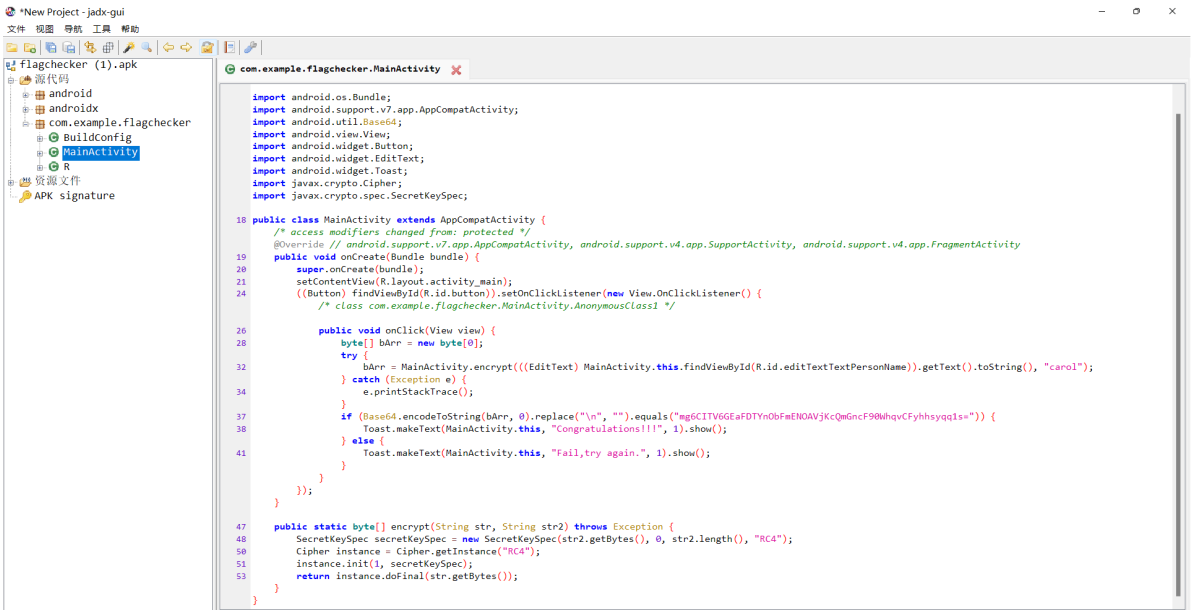
把文件拖进IDA里F5生成伪C代码，观察发现是多了一步异或的Tea加密算法，解的时候注意一下大小端

解密脚本

```c
#include<stdio.h>
int main(void)
{
    unsigned int a[] = {0x48D93488,0x030C144C, 0x52EB78C2,  0xED9CE5ED, 0xAE1FEDE6, 0xBA5A126D,0xCF9284AA,  0x65E0F2E3  };//顺序跟大小端都要注意改一下
    unsigned int v5,v6;
    unsigned int v10[] = { 0x44434241, 0x48474645, 0x4C4B4A49, 0x504F4E4D };//取要用的那些段改一下大小端
    int delta = 0x12345678;
    for (int i = 0; i < 8; i += 2)
    {
        v5 = a[i];
        v6 = a[i + 1];
        int sum = 0x468ACF00;//sum<<5
        for (int j = 0; j < 32; j++)
        {
            v6 -= sum ^ (sum + v5) ^ (v10[0] + (v5 << 4)) ^ (v10[1] + (v5 >> 5));
            v5 -= sum ^ (sum + v6) ^ (v10[2] + (v6 << 4)) ^ (v10[3] + (v6 >> 5));
            sum -= delta;
        }
        a[i] = v5;
        a[i + 1] = v6;
    }
    for (int i = 0; i < 8; i++)
    {
        printf("%x\n", a[i]);//最后将结果的十六进制手动改一下大小端）再转成字符串就是结果了!
    }
    return 0;
}
```

Flag Checker

apk文件在jadx-gui里面打开，找到MainActivity分析（猜）一下发现是base64格式的RC4解密，在cyberchef里面bake一下就能得到flag



猫头鹰不是猫🐱

文件拖进IDA里面分析，F5生成伪C代码找到main然后根据“win”的条件往上找，发现只对v5进行了加密，分析加密函数，观察修改一下数据类型提高可读性，加密过程就是先把a2中的每个元素整除十，再进行矩阵相乘，同样的过程乘不同的二维数组（矩阵）两次得到最后的一维数组，提取数据的过程中也要注意修改数据类型，IDA导出数据（shift+E）时要选择initialized C variable

```
unsigned __int64 __fastcall sub_1347(unsigned int (*a1)[64], unsigned int (*a2)[64][64])
{
  int v3; // [rsp+18h] [rbp-128h]
  int i; // [rsp+1Ch] [rbp-124h]
  int j; // [rsp+20h] [rbp-120h]
  int k; // [rsp+24h] [rbp-11Ch]
  int m; // [rsp+28h] [rbp-118h]
  int n; // [rsp+2Ch] [rbp-114h]
  int v9[66]; // [rsp+30h] [rbp-110h] BYREF
  unsigned __int64 v10; // [rsp+138h] [rbp-8h]

  v10 = __readfsqword(0x28u);
  memset(v9, 0, 0x100uLL);
  for ( i = 0; i <= 63; ++i )
  {
    for ( j = 0; j <= 63; ++j )
      (*a2)[(__int64)i][j] = (signed int)(*a2)[(__int64)i][j] / 10;
  }
  for ( k = 0; k <= 63; ++k )
  {
    v3 = 0;
    for ( m = 0; m <= 63; ++m )
      v3 += (*a1)[m] * (*a2)[(__int64)m][k];
    v9[k] = v3;
  }
  for ( n = 0; n <= 63; ++n )
    (*a1)[n] = v9[n];
  return __readfsqword(0x28u) ^ v10;
}
```

```
; int dword_4140[64][64]        ; int dword_4040[64]
dword_4140      dd 0A2h, 0A0h, dword_4040      dd 25D1
initialized C variable
```

写脚本解密（亿点细节

```python
import numpy as np
v1 = np.array([[162,160,162,161,159,159,159,158,157,157
a2=np.array([39654868,38564788,37998449,36705100,348111
v2=np.array([[150,149,144,134,137,145,141,137,124,109,1
for i in range(64):
    for j in range(64):
        v1[i][j]//=10
for i in range(64):
    for j in range(64):
        v2[i][j]//=10
flag=a2.dot(np.linalg.inv(v2)).dot(np.linalg.inv(v1))
for i in flag:
    print(chr(int(i+0.5)),end="")
```

IoT

饭卡的uno

拖进IDA（）然后就找到了：）

```
aGameF1rst5tep0 db 'game{F1rst_5tep_0F_IOT}',0
```

Web

蛛蛛...嘿嘿♥我的蛛蛛

点到一百关（）检查然后就找到了？）（真的是乱做的所以没有截图dbq）

Misc

欢迎欢迎！热烈欢迎！

关注公众号，好的！