HGAME 第四周部分 WriteUP

· 0x01 virtual_waifu

最后一周惹上点事+题目有点难我就做了一题成功咸鱼...

这题是乍一眼看着很吓人的 VM，但是恰当运用动态调试手段的话其实不难，很容易看出 flag 长度为 24，所以我们先尝试输入 24 个 a

```
61--a
00EFFCDC  B4 BB BA B9 B8 BF BE BD BC A3 A2 A1 A0 A7 A6 A5  椿汗缚窘迹i臆E
00EFFCEC  A4 AB AA A9 A8 AF AE AD 00 00 00 00 00 00 00 00  か  ǒ搏........
```

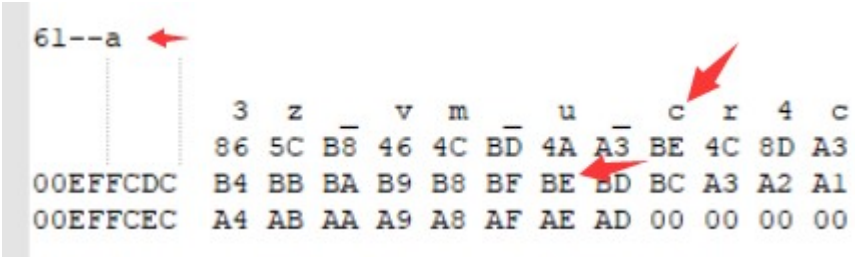
结果有一定规律但是并不好猜测，接下去尝试顺序输入英文字母

```
61 - 79

全是B4

41 - 59

全是94
```

这个结果就很有意思了，我猜测加密过程有一步就是加上字符的偏移，而且密文应该是和 flag 一一对应的，所以做了以下尝试

```
30--0

          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  7  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
005AF8A0  8B 8A 89 88 8F 8E 8D 8C F3 F2 F1 F0 F7 F6 F5 F4  婴增弹率篁精黯豸
005AF8B0  FB FA F9 F8 FF FE FD FC 00 00 00 00 00 00 00 00          ?.......


31

          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  7  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
012FF738  84 8B 8A 89 88 8F 8E 8D 8C F3 F2 F1 F0 F7 F6 F5  剧娈垅帕峤蝰瘅鲴
012FF748  F4 FB FA F9 F8 FF FE FD 00 00 00 00 00 00 00 00  酐  ?  ........

37
          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  7  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
012FFB48  82 81 80 87 86 85 84 8B 8A 89 88 8F 8E 8D 8C F3  倮€嗳屋婴增弹率?
012FFB58  F2 F1 F0 F7 F6 F5 F4 FB 00 00 00 00 00 00 00 00  蝰瘅鲴酐........


42--B
          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  J  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
00CFFC64  95 94 9B 9A 99 98 9F 9E 9D 9C 83 82 81 80 87 86  晹洑櫂煘漾傲亏嗳
00CFFC74  85 84 8B 8A 89 88 8F 8E 00 00 00 00 00 00 00 00  屋婴增弹........


61--a

          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  7  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
00EFFCDC  B4 BB BA B9 B8 BF BE BD BC A3 A2 A1 A0 A7 A6 A5  椿汗缚窘迹i臆E
00EFFCEC  A4 AB AA A9 A8 AF AE AD 00 00 00 00 00 00 00 00  か  ŏ鋪........

62--b

          3  z  _  v  m  _  u  _  c  r  4  c  q  5  d  _  g  0  0  d  _  7  0  b
         86 5C B8 46 4C BD 4A A3 BE 4C 8D A3 BA F3 A1 AB A2 FA F9 A4 AE 80 FD AE
009EFCB4  B5 B4 BB BA B9 B8 BF BE BD BC A3 A2 A1 A0 A7 A6  荡缓垢烤郊"  E
009EFCC4  A5 A4 AB AA A9 A8 AF AE 00 00 00 00 00 00 00 00  イ寐-映........
```

把加密结果复制到每一个结果的上方，找到相同的字节减掉偏移的差就能知道是哪个字母了，比如第 9 个字符是 BE，在全部输入 a 的情况下 BE 的偏移比密文的小 2，就能推出正确的字符是 a+2=c，这样就可以很快推出 flag



至于分析 vm……恕在下无能_(:ʒ」∠)_

顺便总结下这个月参加 HGAME 的所得吧，这个假期也算是学的最多的一个寒假了，以前放假真的不怎么学习……但是学的东西确实有限，战斗力从 5 升到了 8 的程度，最后一周已经有点吃不消了，这周的 WP 一定好好学习一下，除此之外希望开学之后自己也不要懈怠吧