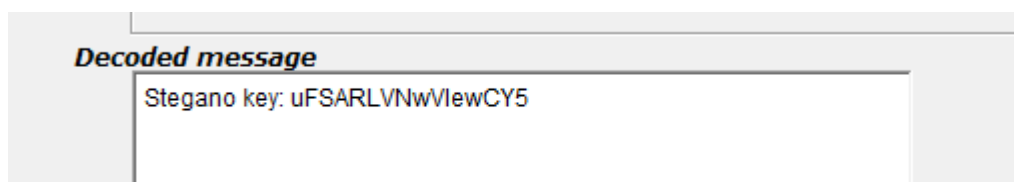


# HGAME2020 WRITE UP

## MISC

### 三重隐写

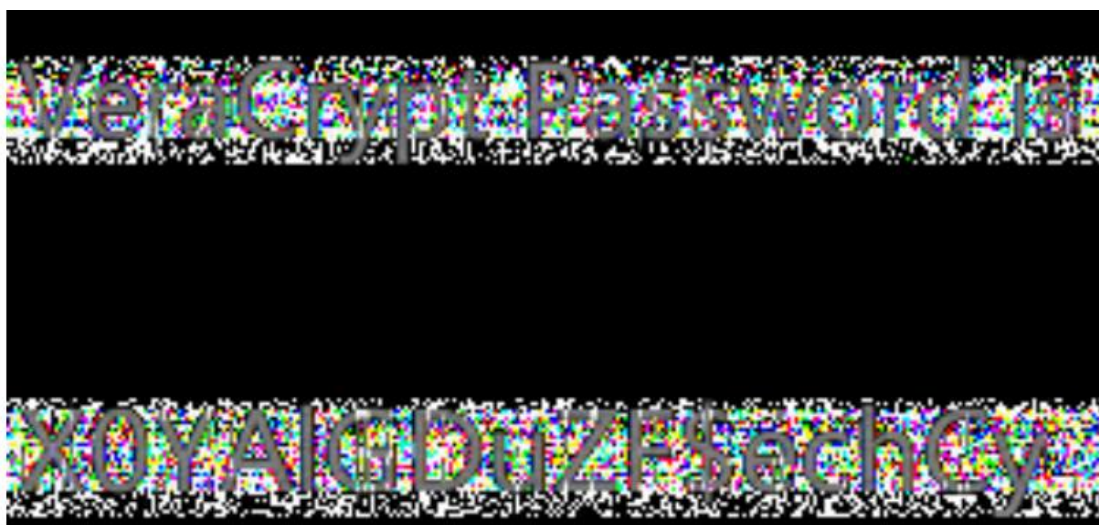
打开压缩包得到 3 个文件，Unlasting 封面图直接扫码得到“AES key: 1ZmmeaLL^Typbcg3”，You know LSB 使用 silenteye 得到



为最后一首歌的隐写密码，使用 MP3stego 得到压缩包密码 Zip Password: VvLvmGjpJ75GdJDP，解开压缩包得到文件用所给软件使用最初得到的 AES 密码解密得到 flag---hgame{j35k#zlewynLC0zfQur!\*H9V\$JiMVWmL}

### 日常

有两张看起来一样的图片，加上文字 blind 和 origin，应该是盲水印，用 blindwatermaster 脚本解得



，.ogg 文件用 binwalk 发现有压缩包，-e 指令取出，水印提示的 VeraCrypt 软件

打开得到三个文件, txt 是 mimikatz 的使用, 查资料后感觉应该是使用 masterkey 解开 cookies, masterkey 在压缩包的 master key file 里, txt 的 NTLM 直接转换为明文密码 happy2020, 逛了好久论坛终于看到关于离线用户 masterkey 但已知明文密码的 masterkey 获取方式, sid 通过 txt 已知, 使用命令 mimikatz # dpapi::masterkey /in:C:\1 /sid:S-1-5-21-3375469711-1363829938-1291733684-1001 /password:happy2020 /protected 获得 masterkey , 使用命令

```
mimikatz 2.2.0 x64 (oe.eo)
.##### mimikatz 2.2.0 (x64) #13362 Jan 4 2020 18:59:26
## ~ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # dpapi::masterkey /in:C:\1 /sid:S-1-5-21-3375469711-1363829938-1291733684-1001 /password:happy2020 /protected

**MASTERKEY**
dwVersion : 00000002 - 2
szGuid : {20d1alc6-d232-40cd-89ec-5678b380920b}
dwFlags : 00000005 - 5
dwMasterKeyLen : 000000b0 - 176
dwBackupKeyLen : 00000090 - 144
dwCredHistLen : 00000014 - 20
dwDomainKeyLen : 00000000 - 0
[masterkey]
**MASTERKEY**
dwVersion : 00000002 - 2
salt : efc278fb18cae03a5f9710d481f090a0
rounds : 000043f8 - 17400
algHash : 0000800e - 32782 (CALG_SHA_512)
algCrypt : 00006610 - 26128 (CALG_AES_256)
pbkey : d348c35ecede1467a1e8baf34609e5bd7a75ae87ef074f9760641f5525596af7c8e85e60a8c9faef66b79382bcbd79a44d33a25bc6271f02e744cc63834e6af2b12ab69653725a0341ec65a1135001a294005c09b0b2380e56c777319989f596e9efcd91030ec214a73eaa53637695c4c15ec35ec4b97daca5885340a5c429be5324f1261d1c996974b32f7698866
[backupkey]
**MASTERKEY**
dwVersion : 00000002 - 2
salt : 8a3989f2df0c972bc9ce35b6fce5b6c
rounds : 000043f8 - 17400
algHash : 0000800e - 32782 (CALG_SHA_512)
algCrypt : 00006610 - 26128 (CALG_AES_256)
pbkey : d171579f6799bb975a1c03f458155777eca5403da9f4a428cecd4c4c388e3257c2384345e03002b6a8164d4e8749a536c0d7b7ade10940a683589ba57632585569ee0ded9aac35f33cd019acd321fdeb83f60400c94f4592df5202cb3bc10a5e0f35ea4b53b46208c03d211ad6ff7
[credhist]
**CREDHIST INFO**
dwVersion : 00000003 - 3
guid : {60333bcc-f0b9-4676-896c-4852eed727cb}

[masterkey] with password: happy2020 (protected user)
key : d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d
sha1 : 14859456844f282211783e88031c13376d7e9e30

mimikatz #
```

dpapi::masterkey /in:C:\Cookies /masterkey:  
d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f968  
4c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d  
/unprotect 得到 flag

```
mimikatz # dpapi::chrome /in:C:\Cookies /masterkey:d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d /unprotected

Host : localhost ( / )
Name : flag
Dates : 2020/1/28 23:37:39 -> 2021/1/28 23:36:26
* volatile cache: GUID: {20d1alc6-d232-40cd-89ec-5678b380920b} KeyHash: 14859456844f282211783e88031c13376d7e9e30
* masterkey : d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d
Cookie: hgame (BOTVnvw8Hxf1ZcCKYf1K1dHf1kQ*cqP4)
```

CRYPTO

RSA?

Linux 直接打开 rsa 文件得到 c,e,q,n 值, e=2, 之前看到过 rabin 加密, 但  $n=p*q+r$  有点难, 想了半天各种方法直到试下直接分解发现 n 分解不了。。。

$$m_p = c^{\frac{1}{4}(p+1)} \bmod p$$

把 p 换成 n 写个脚本得到 flag

```
hgame{eaa5262c-4631-46ef-a97b-53277ab7e1d8}
```

ToyCipher\_XorShift

感觉有点像 CBC 加密模式, BLOCKS 取块, pad 填充, f 为基本的异或位移加密, enc 调用了 f, encrypt 中最初 mid 为 iv, 之后每次变为这次加密的块, (组织语言 ing。。。) 解密只要写出反推的脚本就行了, 对于 enc 加密只要反过来把 block 加密的顺序反过来就行了, 对于 encrypt 先进行异或再 enc 加密, 反过来先解密 enc 再异或就能得到

```
text += XOR(mid, dec(block))
mid = block
```

对于 f 的解密，因为位移后进行异或，解密再异或得到是位移位置的明文，也是用于下一块密文异或解密，所以要不断进行循环（好难组织语言），所以对于 f 解密函数为

```
def f(x, a, shr=True):
    x = x & MASK
    a = a % BITSLENGTH
    s = (1 << a) - 1
    if shr:
        s = s << (BITSLENGTH - a)
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & s) >> a
            s = s >> a
    else:
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & s) << a
            s = s << a
    return x & MASK
```

写脚本得 flag 为

```
hgame{tHi$+4lg0r1thM_i5_3@sY-t0~b2EaK}
```