Woore#0x000012's hgame week2 writeup

CRYPTO

Ancient Recall

把题目交给我的deepseek大人，他会给出答案

这可能对应于逆向后的初始卡牌名称，但需要经过处理。但原题中的初始FATE是5张不同的卡牌，可能包含反转的Major_Arcana卡牌。

综上，最终的FLAG应该是类似hgame{re-The_Fool&...}的形式，具体取决于逆向后的初始卡牌名称。

要解决这个问题，我们需要逆向应用250次变换，从最终的输出还原初始的卡牌组合。以下是解题步骤：

1. **逆向变换分析**：每次变换是将当前元素与下一个元素相加。逆向时需解线性方程组。

2. **应用逆向变换250次**：通过循环逆向操作，还原初始的索引值数组。

3. **确定卡牌名称**：根据索引值判断是否为反转的大阿卡那牌，生成对应的卡牌名称。

```python
Major_Arcana = ["The Fool", "The Magician", "The High Priestess", "The Empress", "The Emperor",
"The Hierophant", "The Lovers", "The Chariot", "Strength", "The Hermit", "Wheel of Fortune", "Ju
stice", "The Hanged Man", "Death", "Temperance", "The Devil", "The Tower", "The Star", "The Moo
n", "The Sun", "Judgement", "The World"]
wands = ["Ace of Wands", "Two of Wands", "Three of Wands", "Four of Wands", "Five of Wands", "Si
x of Wands", "Seven of Wands", "Eight of Wands", "Nine of Wands", "Ten of Wands", "Page of Wand
s", "Knight of Wands", "Queen of Wands", "King of Wands"]
cups = ["Ace of Cups", "Two of Cups", "Three of Cups", "Four of Cups", "Five of Cups", "Six of C
ups", "Seven of Cups", "Eight of Cups", "Nine of Cups", "Ten of Cups", "Page of Cups", "Knight o
f Cups", "Queen of Cups", "King of Cups"]
swords = ["Ace of Swords", "Two of Swords", "Three of Swords", "Four of Swords", "Five of Sword
s", "Six of Swords", "Seven of Swords", "Eight of Swords", "Nine of Swords", "Ten of Swords", "P
age of Swords", "Knight of Swords", "Queen of Swords", "King of Swords"]
pentacles = ["Ace of Pentacles", "Two of Pentacles", "Three of Pentacles", "Four of Pentacles",
"Five of Pentacles", "Six of Pentacles", "Seven of Pentacles", "Eight of Pentacles", "Nine of Pe
ntacles", "Ten of Pentacles", "Page of Pentacles", "Knight of Pentacles", "Queen of Pentacles",
"King of Pentacles"]
tarot = Major_Arcana + wands + cups + swords + pentacles

def reverse_fortune_wheel(current):
    a, b, c, d, e = current
    v1 = (a + b + d - c - e) // 2
    v0 = a - v1
    v2 = b - v1
    v3 = c - v2
    v4 = e - v0
    return [v0, v1, v2, v3, v4]

YOUR_final_Value = [
    25329519520662917748904983691141959172407947049182105205710670853114746750 19,
    25329519520662917748903276660741003578980230131054431788812947003815097952 70,
    25329519520662917748905544592872726604903130315859258544173068376967072335 730,
    25329519520662917748908653282415328853915101626115345140144091742842991390 15,
    25329519520662917748908306626081341560179463763099899341758339139211426093 34
]

current = YOUR_final_Value.copy()
for _ in range(250):
    current = reverse_fortune_wheel(current)

YOUR_initial_FATE = []
for x in current:
    k_normal = x
    k_reversed = x ^ (-1)
    if 0 <= k_reversed < 22:
        YOUR_initial_FATE.append(f"re-{Major_Arcana[k_reversed]}")
    elif 0 <= k_normal < 22:
        YOUR_initial_FATE.append(Major_Arcana[k_normal])
    else:
        YOUR_initial_FATE.append(tarot[x % 78])

FLAG = "hgame{" + "&".join(card.replace(" ", "_") for card in YOUR_initial_FATE) + "}"
print(FLAG)
```

```python
Major_Arcana = ["The Fool", "The Magician", "The High Priestess", "The Empress",
"The Emperor", "The Hierophant", "The Lovers", "The Chariot", "Strength", "The
Hermit", "Wheel of Fortune", "Justice", "The Hanged Man", "Death", "Temperance",
"The Devil", "The Tower", "The Star", "The Moon", "The Sun", "Judgement", "The
World"]
wands = ["Ace of Wands", "Two of Wands", "Three of Wands", "Four of Wands", "Five
of Wands", "Six of Wands", "Seven of Wands", "Eight of Wands", "Nine of Wands",
"Ten of Wands", "Page of Wands", "Knight of Wands", "Queen of Wands", "King of
Wands"]
cups = ["Ace of Cups", "Two of Cups", "Three of Cups", "Four of Cups", "Five of
Cups", "Six of Cups", "Seven of Cups", "Eight of Cups", "Nine of Cups", "Ten of
Cups", "Page of Cups", "Knight of Cups", "Queen of Cups", "King of Cups"]
swords = ["Ace of Swords", "Two of Swords", "Three of Swords", "Four of Swords",
"Five of Swords", "Six of Swords", "Seven of Swords", "Eight of Swords", "Nine of
Swords", "Ten of Swords", "Page of Swords", "Knight of Swords", "Queen of
Swords", "King of Swords"]
pentacles = ["Ace of Pentacles", "Two of Pentacles", "Three of Pentacles", "Four
of Pentacles", "Five of Pentacles", "Six of Pentacles", "Seven of Pentacles",
"Eight of Pentacles", "Nine of Pentacles", "Ten of Pentacles", "Page of
Pentacles", "Knight of Pentacles", "Queen of Pentacles", "King of Pentacles"]
tarot = Major_Arcana + wands + cups + swords + pentacles

def reverse_fortune_wheel(current):
    a, b, c, d, e = current
    v1 = (a + b + d - c - e) // 2
    v0 = a - v1
    v2 = b - v1
    v3 = c - v2
    v4 = e - v0
    return [v0, v1, v2, v3, v4]

YOUR_final_Value = [
    2532951952066291774890498369114195917240794704918210520571067085311474675019,
    2532951952066291774890327666074100357898023013105443178881294700381509795270,
    2532951952066291774890554459287276604903130315859258544173068376967072335730,
    2532951952066291774890865328241532885391510162611534514014409174284299139015,
    2532951952066291774890830662608134156017946376309989934175833913921142609334
]

current = YOUR_final_Value.copy()
for _ in range(250):
    current = reverse_fortune_wheel(current)

YOUR_initial_FATE = []
for x in current:
    k_normal = x
    k_reversed = x ^ (-1)
    if 0 <= k_reversed < 22:
        YOUR_initial_FATE.append(f"re-{Major_Arcana[k_reversed]}")
    elif 0 <= k_normal < 22:
        YOUR_initial_FATE.append(Major_Arcana[k_normal])
    else:
        YOUR_initial_FATE.append(tarot[x % 78])
```

```
FLAG = "hgame{" + "&".join(card.replace(" ", "_") for card in YOUR_initial_FATE)
+ "}"
print(FLAG)
```

Fence 1

deepseek大人真是强强又大大呢

MISC

Computer cleaner plus

拿到附件导入VM中，根据题目提示"发现自己的电脑还在遭受黑客的控制"去进程里面查找，发现ps指令被禁用了，而top还可以用，然后在top里面翻了半天，又去/proc翻了好几天，结果什么都没有发现，后来想着去看看ps怎么个事，但是不知道怎么想的想要ls /bin/ps而且还手误打成了cat /bin/ps，然后就出后门应用了

Figure 2

真是意意又外外呢

WEB

Level 21096 HoneyPot && Level 21096 HoneyPot_Revenge

将代码喂给chatgpt大人，他说可能存在CVE-2024-21096漏洞，然后去万能的互联网上搜索，找到了出题大人的博客嘻嘻，CVE-2024-21096 mysqldump命令注入漏洞简析 | Ec3o

然后照着出题大人的博客做，又有题目提示"2. 容器内置有 `/writeflag` 命令，会把预设的 `flag` 写入到 `/flag` 位置进行读取。"于是将version中的插入命令改成/writeflag，随后进行两天两夜的编译，最终终于是成功安装上了（还花了大洋去搞了个新服务器过来呜呜呜），然后进行连接，发现他又连接不上，研究了一番发现他不支持远程root登录┳┳＿┳┳，所以还得创建一个允许任意ip登录的用户用于连接，参照：mysql创建用户任意ip地址登录 – CSDN文库

随后就可以连接成功啦，然后访问/flag路由，就可以拿到心心念念的flag啦

这题是折折又磨磨、有有又趣趣呢