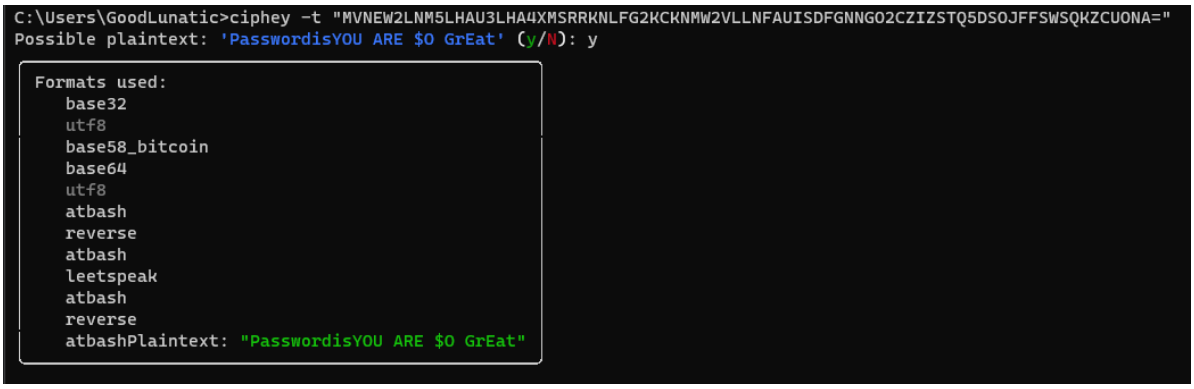
Misc——Citanul的大秘宝WP

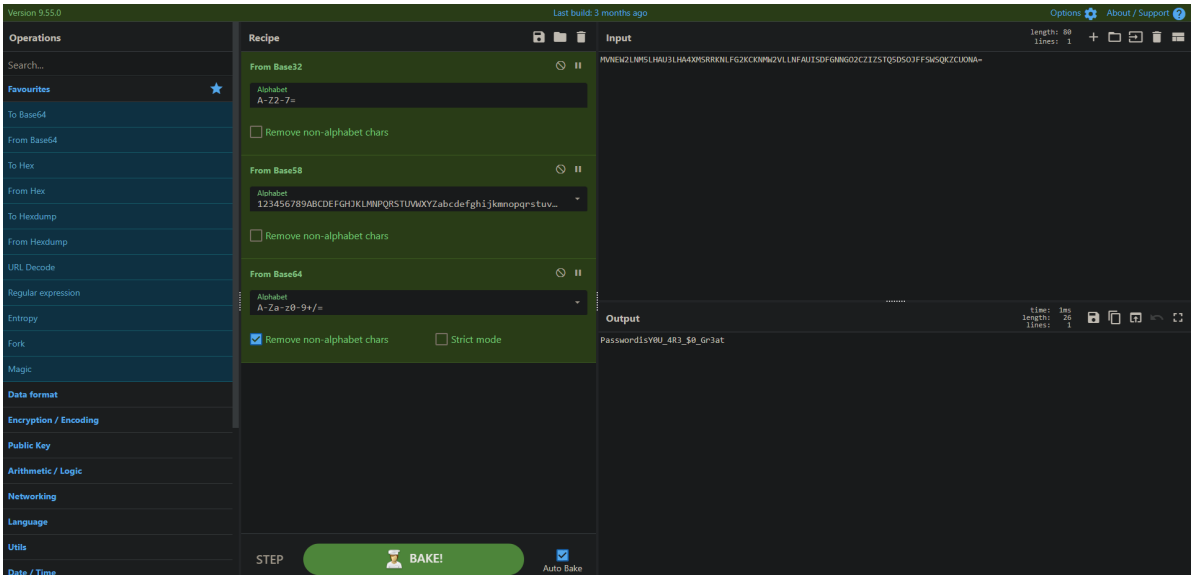
flag：zjnuctf{7abe404919c927b3dc71b93102227389}

#步骤一
首先该压缩包的密码是A1na#
SHA2-256加密算法加密后的结果是
08af717376f7f71b9525f4f76fb0bfc8b12a210a5653e87989bf7f46e96640c6
解法一：直接用Advanced Archive Password Recovery限制长度爆破压缩包密码（几秒就出了）
解法二：用hashcat爆破（也是秒出）
hashcat --custom-charset1 ?d?l?u?s -a 3 -m 1400
08af717376f7f71b9525f4f76fb0bfc8b12a210a5653e87989bf7f46e96640c6 ?1?1?1?1?1
非预期解：CMD5加钱购买

#步骤二
压缩包开出来有一个加密的word还有一个MP3Stego隐写过的mp3文件
可以大胆猜测word的密码就藏在在这个mp3文件中
使用MP3Stego破解出隐写的文本（这里的这个MP3Stego是没有密码的，要输入密码时直接回车就行）

#步骤三
MP3stego Decode后得到一段base混合编码后的密文
#加密过程如下
明文：PasswordisYOU_4R3_$O_Gr3at
base64：UGFzc3dvcmRpc1kwVV8OUjNfJDBfR3IzYXQ=
base58:eZKimgVpSk89vJ1SVSiBSYmUkiADHe3ZghYFe8trrJYZPVEG4
base32:MVNEW2LNM5LHAU3LHA4XMSRRKNLFG2KCKNMW2VLLNFAUISDFGNNGO2CZIZSTQ5DSOJFFSWSQKZCUONA=
#随波逐流应该是出不来的，用CyberChef中的magic或者ciphey都是秒出（这里ciphey可能有点问题，把下划线自动删去了，还是建议用CyberChef）





#步骤四

得到word的密码后打开word

前面的背景知识仅作了解即可，主要是要看后面的两段数据

3460转为十六进制后是0x0D84

4230转为十六进制后是0x1086

可见表示余额的十六进制数据是小端序存储的，然后很明显最后一位就是校验位

这里可能需要一点点的经验、尝试和猜测了

0x0D+0x84-0x15=0x7C

0x10+0x86-0x1A=0x7C

所以我们到这里就知道最后一位校验位是怎么生成的了

所以当余额为600时，这一行的数据就是

60EA00000000160B1A0832030C0000CE

所以最后的flag就是：zjnuctf{7abe404919c927b3dc71b93102227389}

#后来加的Hint

Hint就在这里，但是你看不见.txt 这个文件考察的是零宽字符，直接在线网站解密即可

零宽度字符的Unicode隐写术

这是纯文本隐写术，带有Unicode的零宽度字符。
零宽度字符插入文本中。

JavaScript库在下面。
http://330k.github.io/misc_tools/unicode_steganography.js

文本隐写术示例中的文本

原文: 清除 (长度: 377)

《进击的巨人》（日语：進撃の巨人）是日本漫画家谏山创创作的漫画作品。漫画于2009年9月至2021年4月间在讲谈社《别册少年Magazine》上连载，单行本全34卷。故事建立在人类与巨人之间的冲突，人类居住在由高墙包围的城市，对抗墙外会吃人的巨人，并寻找著关于巨人的答案。漫画系列截至2021年6月发行至第34

隐藏文字: 清除 (长度: 40)

偷偷地告诉你，Lunatic为了减小难度，这个Mp3stego隐写是没有密码的。

加密 »

« 解密

隐写文本: 清除 (长度: 697)

《进击的巨人》（日语：進撃の巨人）是日本漫画家谏山创创作的漫画作品。漫画于2009年9月至2021年4月间在讲谈社《别册少年Magazine》上连载，单行本全34卷。故事建立在人类与巨人之间的冲突，人类居住在由高墙包围的城市，对抗墙外会吃人的巨人，并寻找著关于巨人的答案。漫画系列截至2021年6月发行至第34卷，在日本国内累计发行量突破8,600万册，在海外则突破1,200万册的销量，实体书和电子书的世界累计发行量破亿。本作在商业上获得巨大的成功，作品被改编成多项衍生作品，其改编动画让原作更受瞩目，进而在亚洲及欧美取得高人气。2015荣获SUGOI JAPAN Award漫画部门首奖、动画部门第7名，讲谈社于2018年10月30日正式宣布与华纳兄弟影业达成协议，预计将推出好莱坞真人版电影，并由曾执导过电影《小丑回魂》的安德雷斯·马希提担任导演。

将Stego文本下载为文件

隐写术的零宽度字符:

- [ ] U+200A ZERO WIDTH SPACE
- [ ] U+200B ZERO WIDTH SPACE
- [x] U+200C ZERO WIDTH NON-JOINER
- [x] U+200D ZERO WIDTH JOINER
- [ ] U+200E LEFT-TO-RIGHT MARK
- [ ] U+200F LEFT-TO-RIGHT MARK
- [ ] U+202A LEFT-TO-RIGHT EMBEDDING
- [x] U+202C POP DIRECTIONAL FORMATTING
- [ ] U+202D LEFT-TO-RIGHT OVERRIDE
- [ ] U+2062 INVISIBLE TIMES
- [ ] U+2063 INVISIBLE SEPARATOR
- [x] U+FEFF ZERO WIDTH NO-BREAK SPACE