First of all, since the binary is stripped of symbols, we try to CTRL + f “main” to find the **main_main** function. Upon closer inspection, it seems like a 32 character passphrase is used to encode a string via AES-ECB. After running the binary we see the ciphertext is **925305baa4c16cec6bdf480763cad98a**. I tried to decode it using the passphrase I got:ssssssss

```python
from Crypto.Cipher import AES
import binascii
import hashlib
passphrase = "thisis32bitlongpassphraseimusing".encode('utf-8')
ciphertext_hex = "925305baa4c16cec6bdf480763cad98a"
ciphertext = binascii.unhexlify(ciphertext_hex)
cipher = AES.new(passphrase, AES.MODE_ECB)
decrypted = cipher.decrypt(ciphertext)
decrypted_text = decrypted.decode('utf-8')
sha256_hash = hashlib.sha256(decrypted_text.encode('utf-8')).hexdigest()
print(decrypted_text)
print(f"ctf{{{sha256_hash}}}")
```

This program reveals that the plaintext was in fact in the source code, and was the first 16 characters of the text sent to the AES encryption. I preferred to make a decryption of the ciphertext the binary gave me to prevent a red herring.

Either way, the flag is ctf{sha256(plaintext)}

Made with love by: AndreiCat