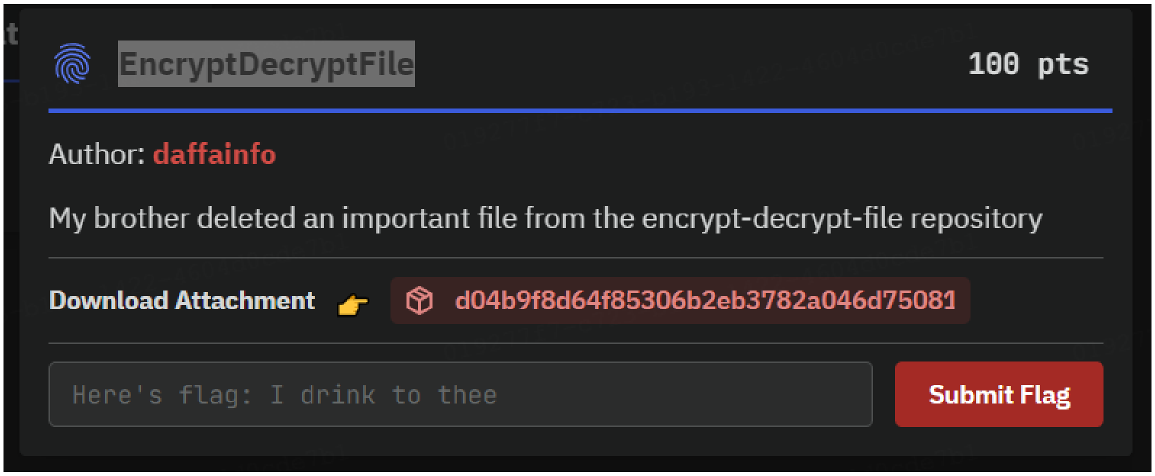
EncryptDecryptFile - 100 pts (recover Mercurial repository)



EncryptDecryptFile 100 pts

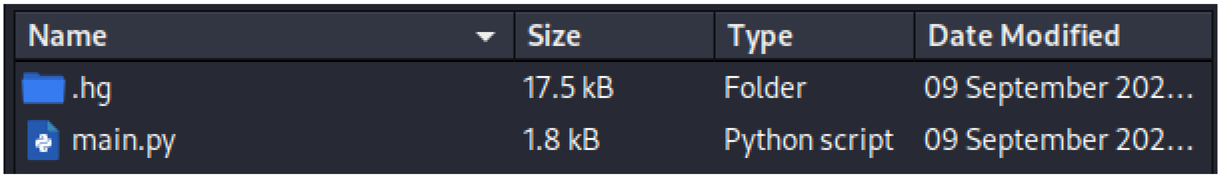
Author: daffainfo

My brother deleted an important file from the encrypt-decrypt-file repository

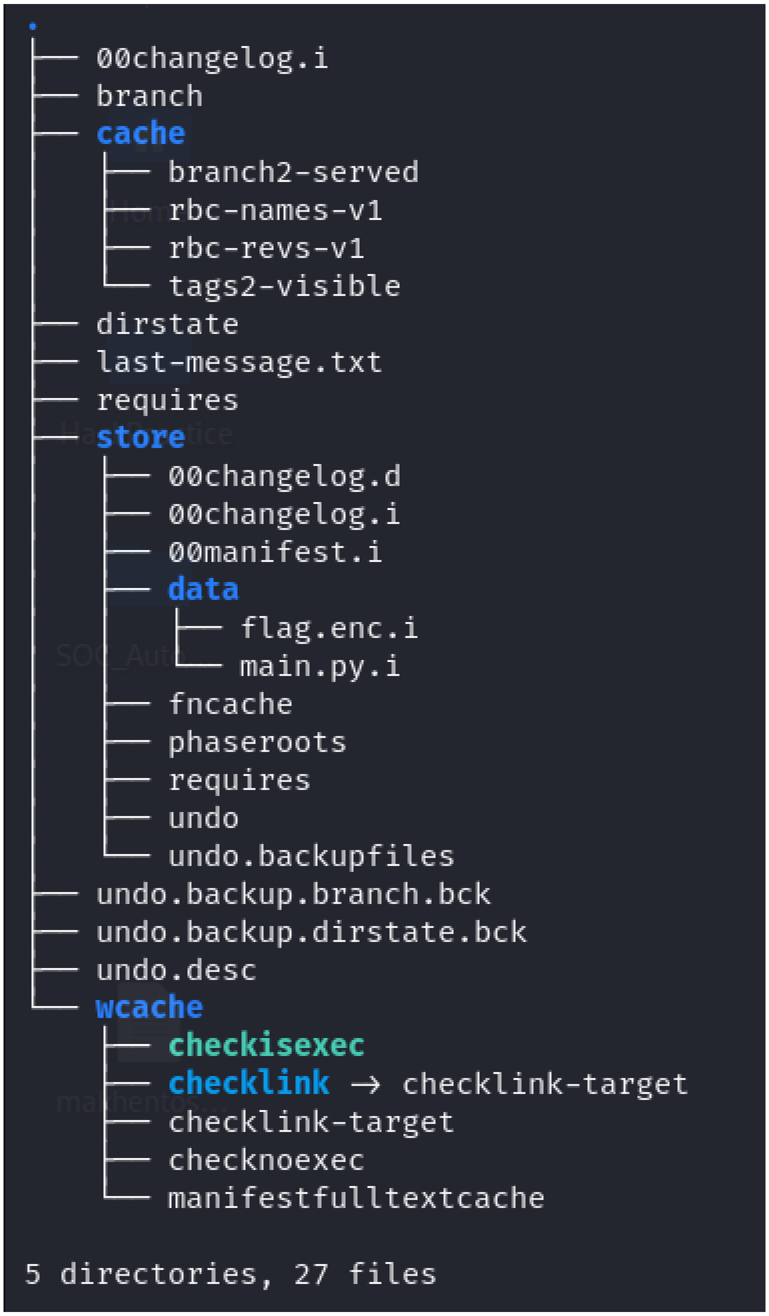
Download Attachment d04b9f8d64f85306b2eb3782a046d75081

Here's flag: I drink to thee

We are provided with `.hg` which is Mercurial metadata directory and Python code file. `.hg`directory contains the necessary files and metadata to track the history, revisions, and configuration of the Mercurial repository.



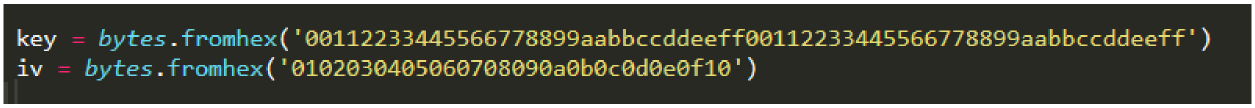
Name	Size	Type	Date Modified
.hg	17.5 kB	Folder	09 September 202…
main.py	1.8 kB	Python script	09 September 202…



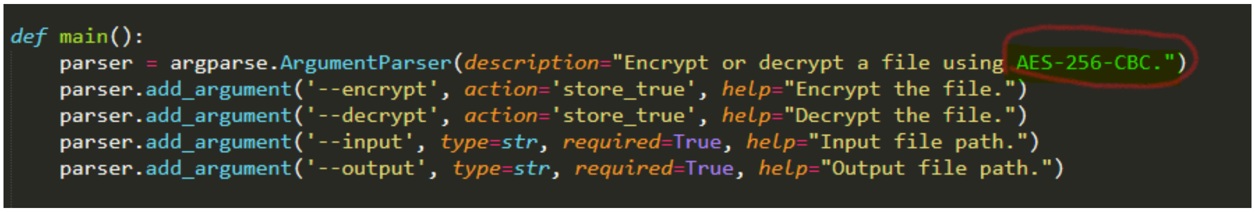
```
.
├── 00changelog.i
├── branch
├── cache
│   ├── branch2-served
│   ├── rbc-names-v1
│   ├── rbc-revs-v1
│   └── tags2-visible
├── dirstate
├── last-message.txt
├── requires
├── store
│   ├── 00changelog.d
│   ├── 00changelog.i
│   ├── 00manifest.i
│   ├── data
│   │   ├── flag.enc.i
│   │   └── main.py.i
│   ├── fncache
│   ├── phaseroots
│   ├── requires
│   ├── undo
│   └── undo.backupfiles
├── undo.backup.branch.bck
├── undo.backup.dirstate.bck
├── undo.desc
└── wcache
    ├── checkisexec
    ├── checklink → checklink-target
    ├── checklink-target
    ├── checknoexec
    └── manifestfulltextcache

5 directories, 27 files
```

.hg directory tree

After reviewing the `main.py` file I understood that this is an encryption-decryption program. The code contains **encryption keys** and **method** information which might be handy in solving this task.

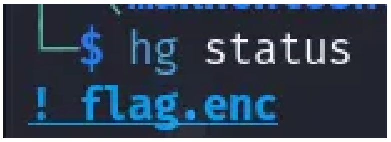


```
key = bytes.fromhex('00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff')
iv = bytes.fromhex('0102030405060708090a0b0c0d0e0f10')
```



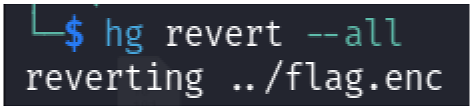
```
def main():
    parser = argparse.ArgumentParser(description="Encrypt or decrypt a file using AES-256-CBC.")
    parser.add_argument('--encrypt', action='store_true', help="Encrypt the file.")
    parser.add_argument('--decrypt', action='store_true', help="Decrypt the file.")
    parser.add_argument('--input', type=str, required=True, help="Input file path.")
    parser.add_argument('--output', type=str, required=True, help="Output file path.")
```

Let's get back to our `.hg` directory. Since we are told that the file has been deleted, we can check the status of files in the repository using command `hg status` .



```
└─$ hg status
! flag.enc
```

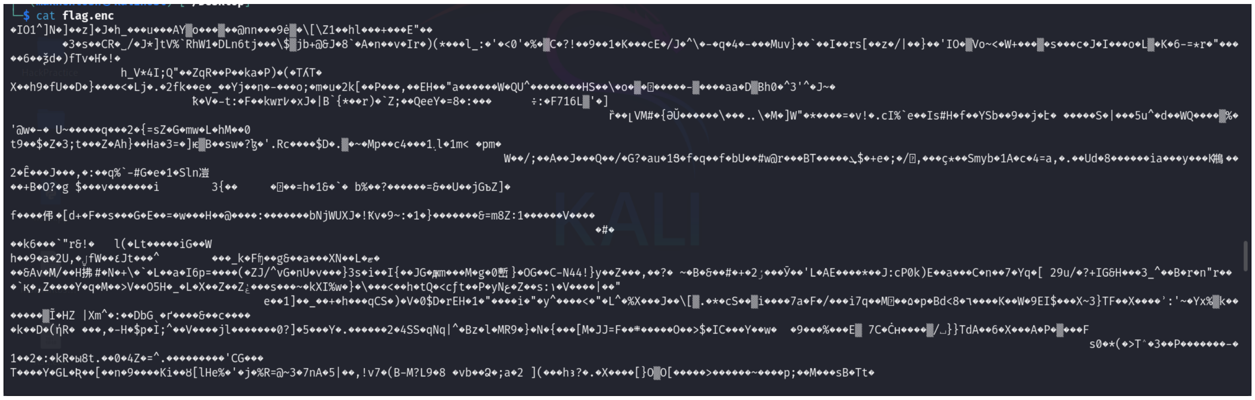
In the output we see `flag.enc` file and `!` sign indicating that the file is missing. Therefore we learned which file has been deleted, most likely this is our flag. We can revert this missed file using the command `hg revert -all` .



```
└─$ hg revert --all
reverting ../flag.enc
```

There it is. The `flag.enc` file is recovered.

If we open this file we can see bunch of random symbols. This is an encrypted text.

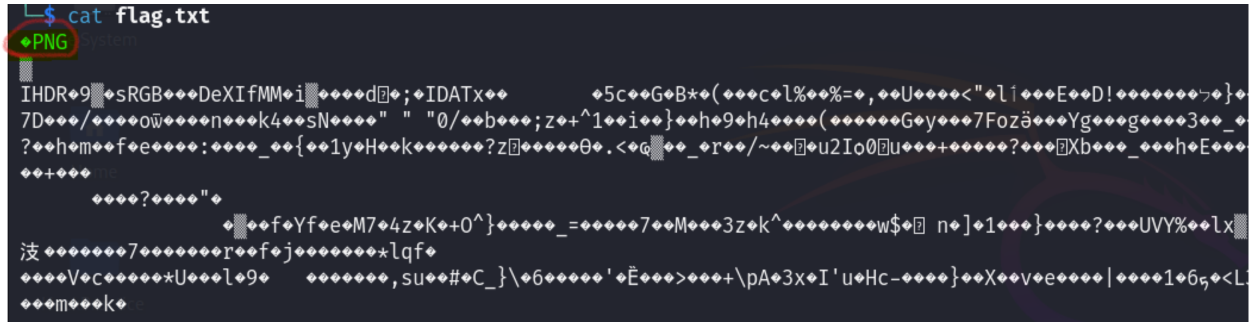


```
└─$ cat flag.enc
```

We know the **encryption key**, **IV**, and **encryption method** from analyzing the `main.py` code. Use `openssl` to decrypt this file.

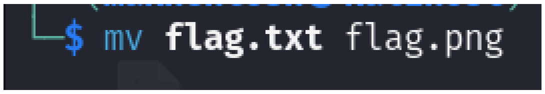
`openssl enc -d -aes-256-cbc -in flag.enc -out flag.txt -K 00112233445566778899aabbccddeeff00112233445566778899aabbccddeeff -iv 0102030405060708090a0b0c0d0e0f10` .

The decryption is successful. After checking the `flag.txt` content I realized that this is a PNG image.

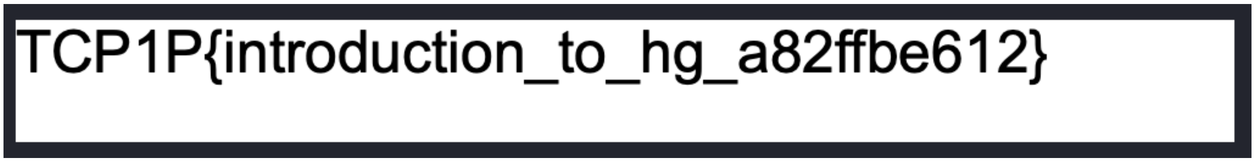


```
└─$ cat flag.txt
�PNG
▒
IHDR�9▒�sRGB���DeXIfMM�i▒����d�;�IDATx��       �5c��G�B*�(���c�l%��%=�,��U�����<"�lί���E��D!�������ㄱ�}�
7D���/����ow̄����n���k4��sN����" " "0/��b���;z�+^1��i��}��h�9�h4����(������G�y���7Fozə���Yg���g����3��_�
?��h�m��f�e�����:����_��{��1y�H��k������?z������θ�.<�ɋ▒��_�r��/~���u2Iọ0u���+�����?���Xb���_���h�E���
��+���
      ����?����"�
                  �▒��f�Yf�e�M7�4z�K�+O^}�����_=�����7��M���3z�k^��������w$� n�]�1���}����?���UVY%��lx▒
汥�������7�������r��f�j��������*lqf�
����V�c������*U���l�9�   ��������,su��#�C_}\�6������'�Ȅ���>����+\pA�3x�I'u�Hc-����}��X��v�e�����|����1�6ҁ�<L
���m����k�
```

Rename this .txt file to .png and open it up.



```
└─$ mv flag.txt flag.png
```



TCP1P{introduction_to_hg_a82ffbe612}

Congratulations, the flag is obtained!