BabyEncryption-hackthebox

the CTF starts with downloading a zip file containing 2 files:

1. python file that is used to encrypt the second file
2. encrypted file

```python
import string
from secret import MSG

def encryption(msg):
    ct = []
    for char in msg:
        ct.append((123 * char + 18) % 256)
    return bytes(ct)

ct = encryption(MSG)
f = open('./msg.enc','w')
f.write(ct.hex())
f.close()
```

we can see that the encryption is using modulo function that can be inverted and decrypted, we need to find the inverse of 123 mod 256.

$$179 \equiv 123^{-1} \pmod{256}$$
$$179 \times 123 \equiv 1 \pmod{256}$$

using the same way they encrypted the file we can now decrypt it.

```python
# 179 is the inverse of 123 mod 256
def decription(msg):
    de = []
    for char in msg:
        char = char - 18
        char = (char * 179) % 256
        de.append(char)
    print(bytes(de))


if __name__ == '__main__':
    with open("msg.enc") as f:
        b = bytes.fromhex(f.read())
        decription(b)
```

this will print:

```
b'Th3 nucl34r w1ll 4rr1v3 0n fr1d4y.\nHTB{l00k_47_y0u_r3v3rs1ng_3qu4710n5_c0ngr475}'
```

so the flag is:

HTB{l00k_47_y0u_r3v3rs1ng_3qu4710n5_c0ngr475}