BabyEncryption

CHALLENGE DESCRIPTION

You are after an organised crime group which is responsible for the illegal weapon market in your country. As a secret agent, you have infiltrated the group enough to be included in meetings with clients. During the last negotiation, you found one of the confidential messages for the customer. It contains crucial information about the delivery. Do you think you can decrypt it?

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# ls
BabyEncryption.ctb  BabyEncryption.zip
```

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# unzip BabyEncryption.zip
Archive:  BabyEncryption.zip
[BabyEncryption.zip] chall.py password:
  inflating: chall.py
  inflating: msg.enc
```

After unzipping the file we have two more files, “chall.py” which is the python script to decrypt the cipher text & “msg.enc” which contains the cipher text.

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# cat chall.py
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()


┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# cat msg.enc
6e0a9372ec49a3f6930ed8723f9df6f6720ed8d89dc4937222ec7214d89d1e0e352ce0aa6ec82bf622227bb70e7fb7352249b7d893c493d8539dec8fb7935d490e7f9d22ec89b7a322ec8fd80e7f8921
```

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# chmod +x chall.py
```

If you execute the script it will throw errors as follows…

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# python chall.py
Traceback (most recent call last):
  File "chall.py", line 2, in <module>
    from secret import MSG
ImportError: No module named secret
```

After wasting few seconds in fixing the error I give up and decided to create a script based on chall.py

decrypt.py

```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

def decryption(msg):
    pt = []
    for char in msg:
        char = char - 18
        char = 179 * char % 256
        pt.append(char)
    return bytes(pt)
with open('msg.enc') as f:
    ct = bytes.fromhex(f.read())

pt = decryption(ct)
print(pt)
```

```
┌──(root💀kali)-[/Documents/htb/challenge/crypto/BabyEncryption]
└─# python3 decrypt.py
b'Th3 nucl34r w1ll 4rr1v3 0n fr1d4y.\nHTB{l00k_47_y0u_r3v3rs1ng_3qu4710n5_c0ngr475}'
```