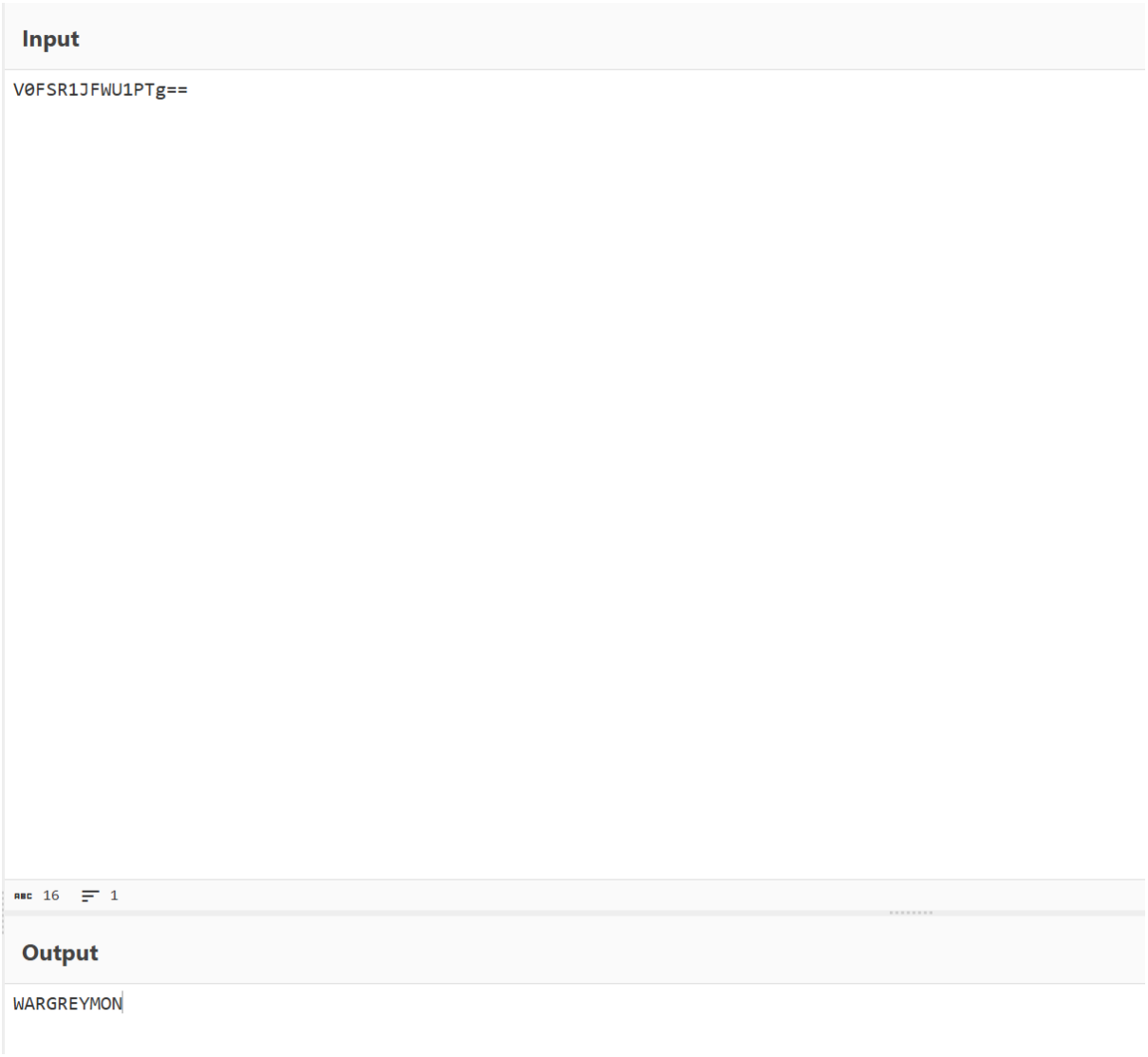
2024 JFS secret_message write up

제공된 secret.txt 파일에서 Message와 KEY 정보를 얻을 수 있다.



Message는 base64 디코딩한 결과 WARGREYMON 이라는 문자열임을 알 수 있다.

따라서 이 정보를 가지고 sha256을 사용한 HMAC을 구성할 수 있다.

```python
# -*- coding: utf-8 -*-

import hmac
import hashlib
import binascii

#아래는 송신자와 수신자가 사전에 공유해야할 비밀키
key = bytes.fromhex("E49756B4C8FAB4E48222A3E7F3B97CC3")
message = b"WARGREYMON"

#key와 SHA256 해싱 알고리즘을 사용하여 HMAC 메시지 생성
hmac_msg = hmac.new(key, message, hashlib.sha256)

#만들어진 HMAC 메시지 출력
print ("HMAC:", hmac_msg.hexdigest())
```

위와 같이 코드를 작성하면 HMAC을 얻을 수 있다.

정답

```
JFS{eb8b6165369814a2fecc7711ce041bcf6c2dd04b16a2d3487b4181bc908e0731}
```