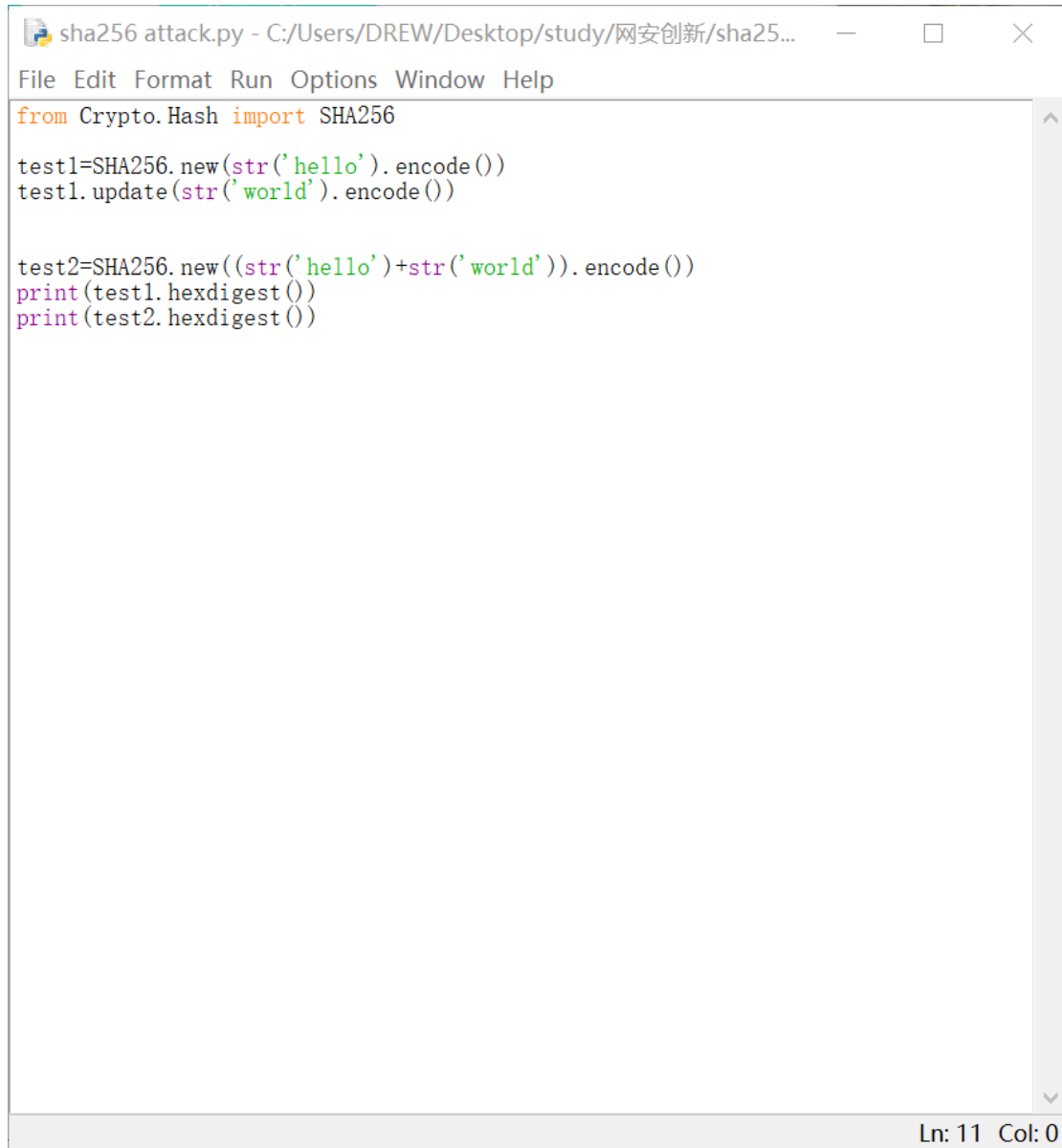


SHA256 长度扩展攻击

针对 md 结构的哈希函数，可以使用长度扩展攻击进行伪造。如已知 hash (hello)，则可以以 hash (hello) 为初始向量，对 hash (helloworld) 进行伪造。

即 hash (IV, helloworld) = hash (hash (IV, hello), world)。

使用 SHA256 算法进行伪造，使用了 python 中的库函数。

A screenshot of a Python script editor window titled 'sha256 attack.py - C:/Users/DREW/Desktop/study/网安创新/sha25...'. The window has a menu bar with 'File', 'Edit', 'Format', 'Run', 'Options', 'Window', and 'Help'. The code inside is as follows:

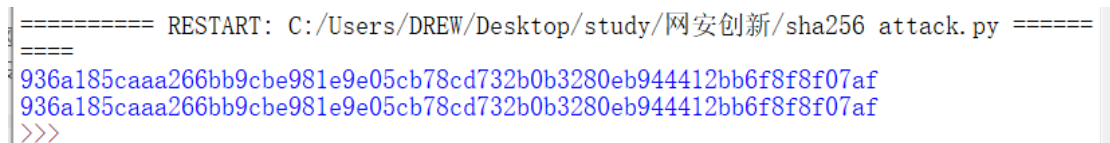
```
from Crypto.Hash import SHA256

test1=SHA256.new(str('hello').encode())
test1.update(str('world').encode())

test2=SHA256.new((str('hello')+str('world')).encode())
print(test1.hexdigest())
print(test2.hexdigest())
```

The status bar at the bottom right shows 'Ln: 11 Col: 0'.

结果：

A screenshot of a terminal window showing the output of the script. The output is as follows:

```
===== RESTART: C:/Users/DREW/Desktop/study/网安创新/sha256 attack.py =====
=====
936a185caaa266bb9cbe981e9e05cb78cd732b0b3280eb944412bb6f8f8f07af
936a185caaa266bb9cbe981e9e05cb78cd732b0b3280eb944412bb6f8f8f07af
>>>
```

可以看到二者相同，伪造成功。