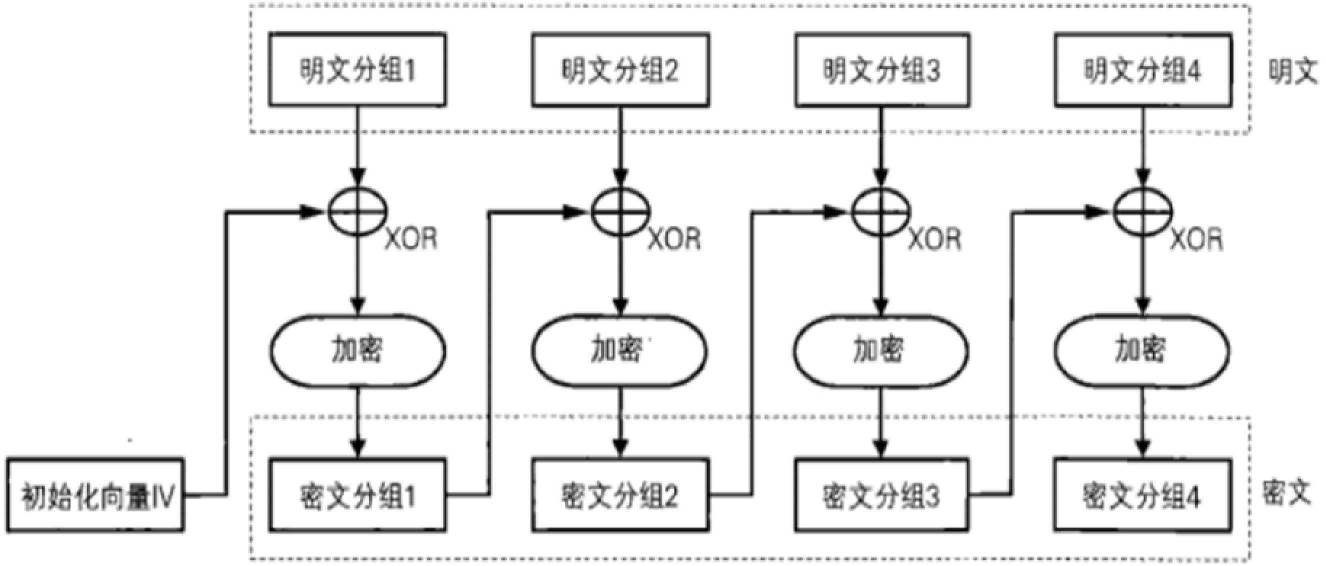
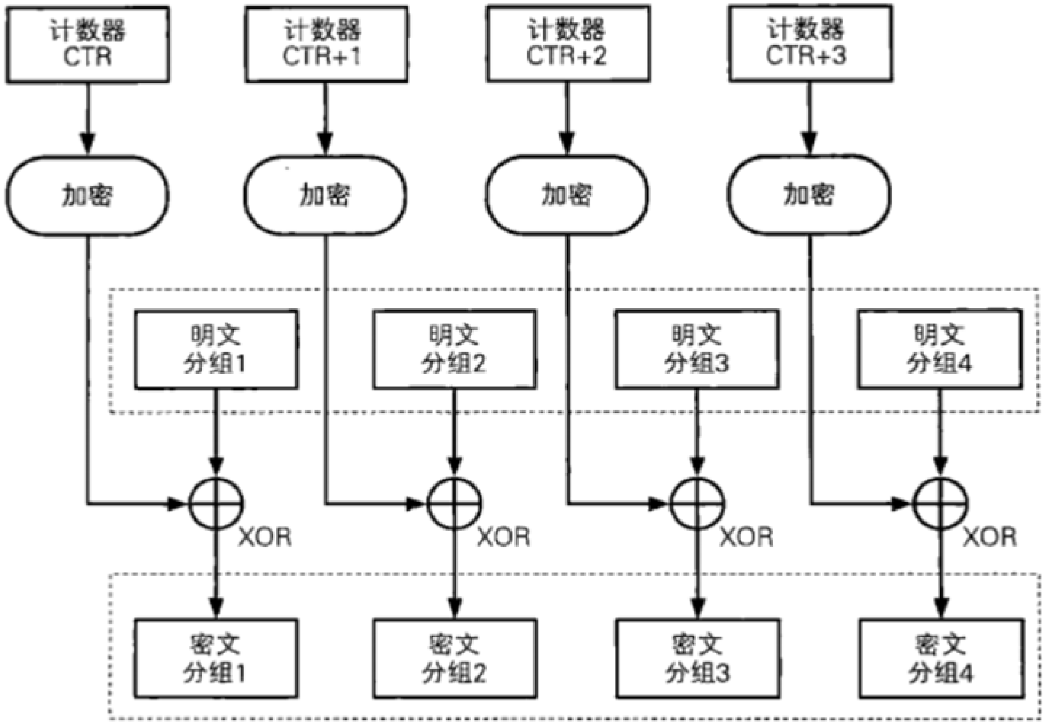
密码学课程

CBC模式的加密



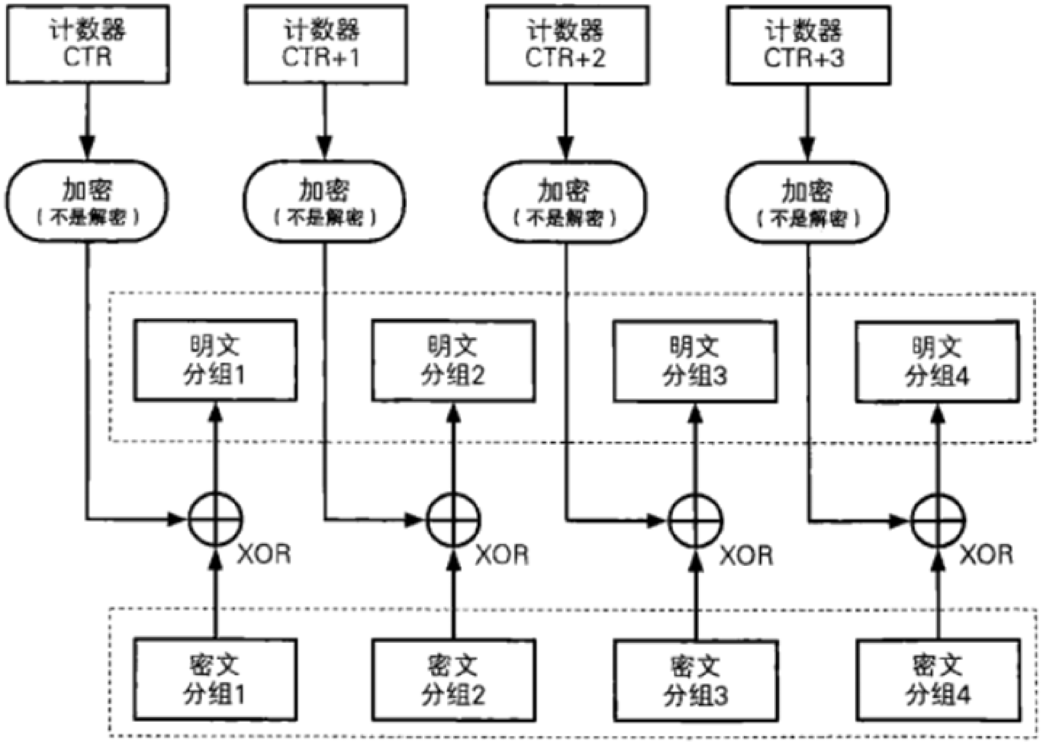
密码学课程

CTR模式的加密



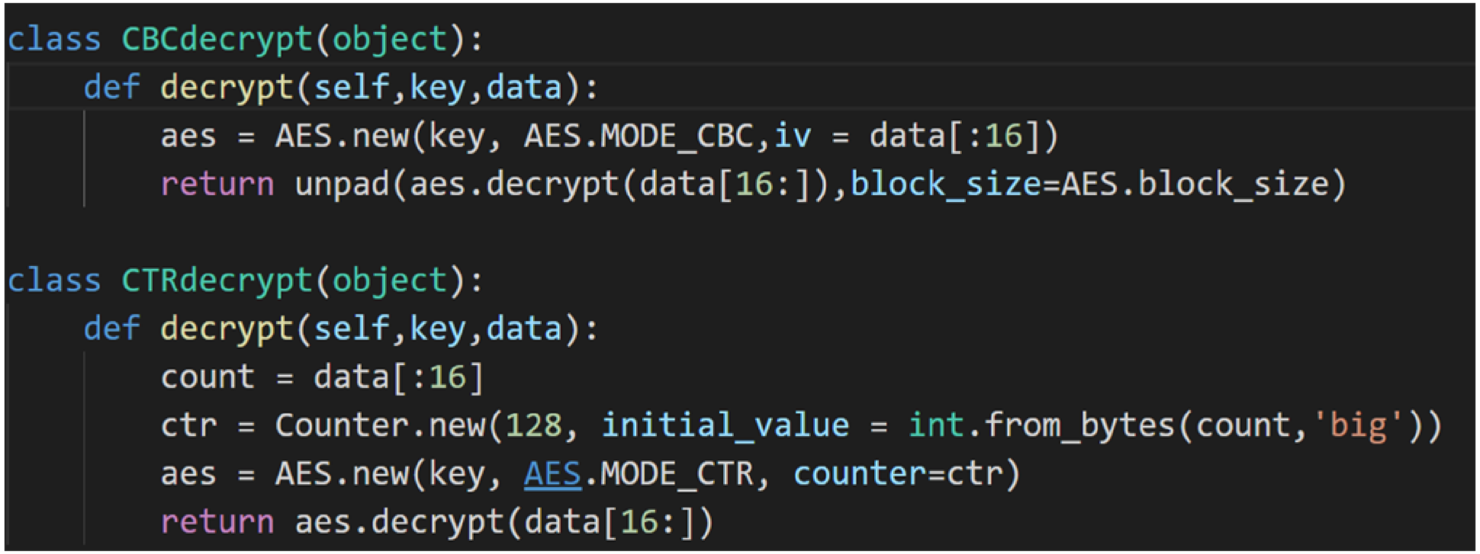
密码学课程

CTR模式的解密



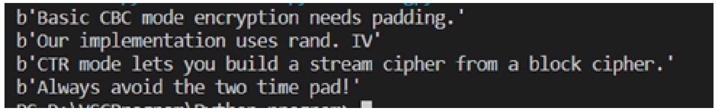
密码学课程

Python解密代码(使用pycrypto库)



```python
class CBCdecrypt(object):
    def decrypt(self,key,data):
        aes = AES.new(key, AES.MODE_CBC,iv = data[:16])
        return unpad(aes.decrypt(data[16:]),block_size=AES.block_size)

class CTRdecrypt(object):
    def decrypt(self,key,data):
        count = data[:16]
        ctr = Counter.new(128, initial_value = int.from_bytes(count,'big'))
        aes = AES.new(key, AES.MODE_CTR, counter=ctr)
        return aes.decrypt(data[16:])
```



```
b'Basic CBC mode encryption needs padding.'
b'Our implementation uses rand. IV'
b'CTR mode lets you build a stream cipher from a block cipher.'
b'Always avoid the two time pad!'
PS D:\VSCProgram\Python program> 
```