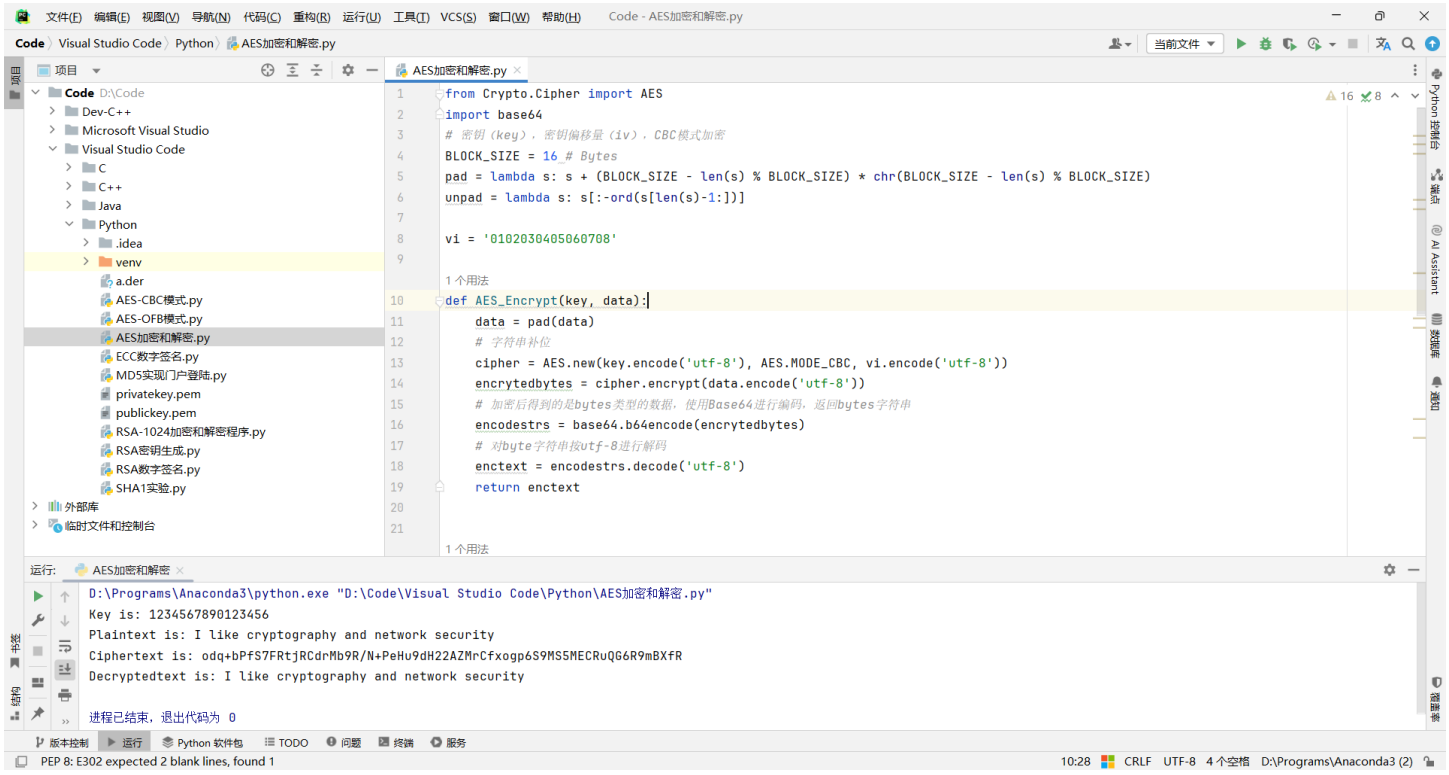

图 1-1 AES 加密和解密

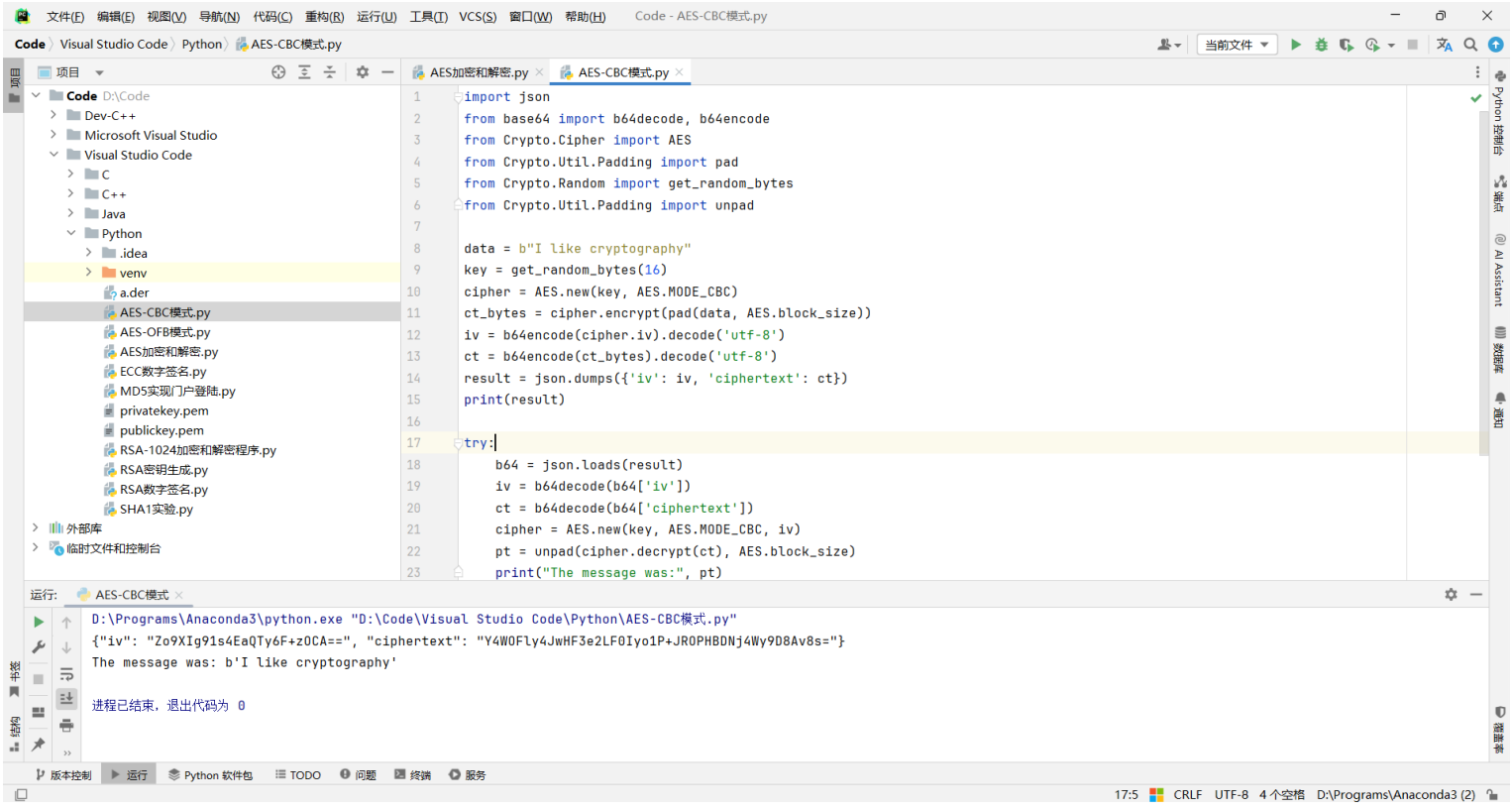

图 1-2 AES-CBC 模式

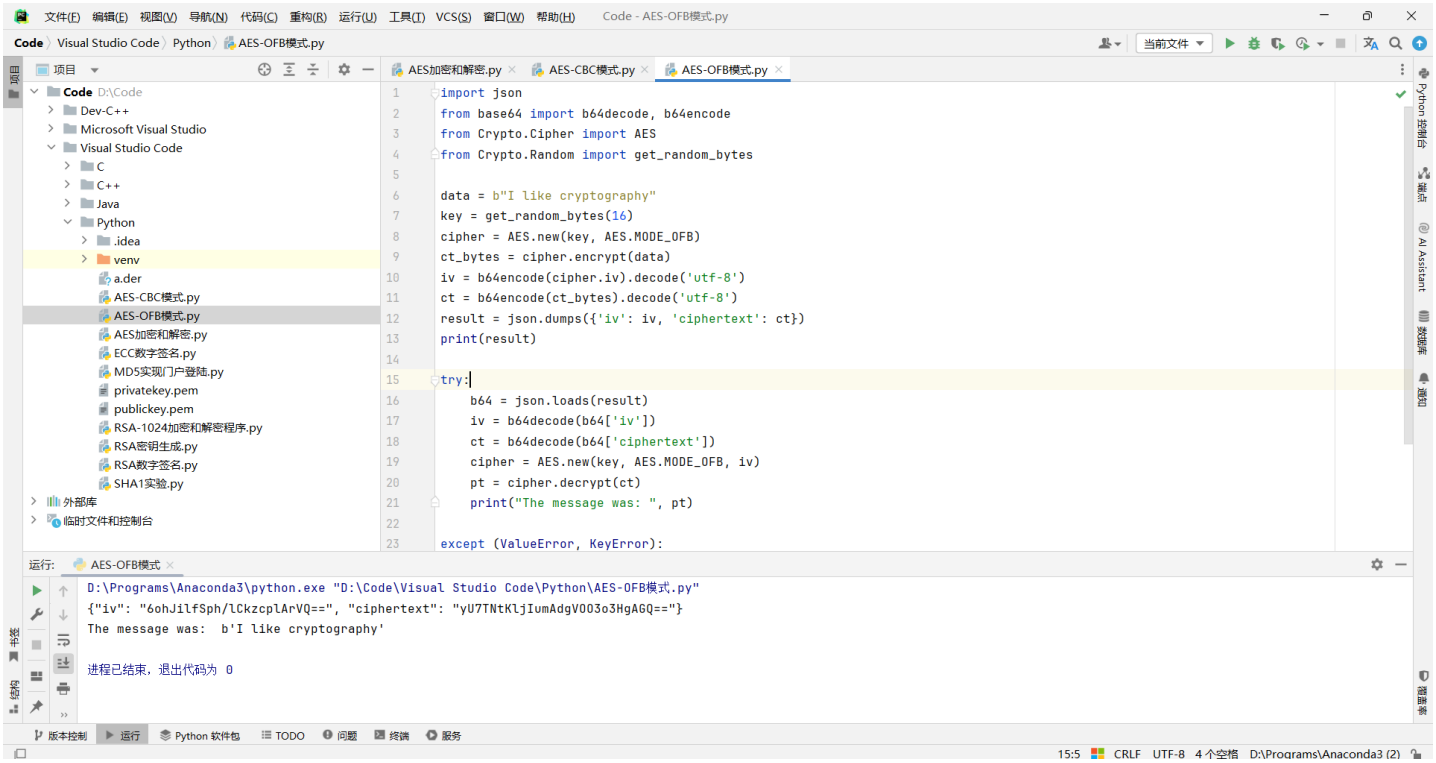

图 1-3 AES-OFB 模式

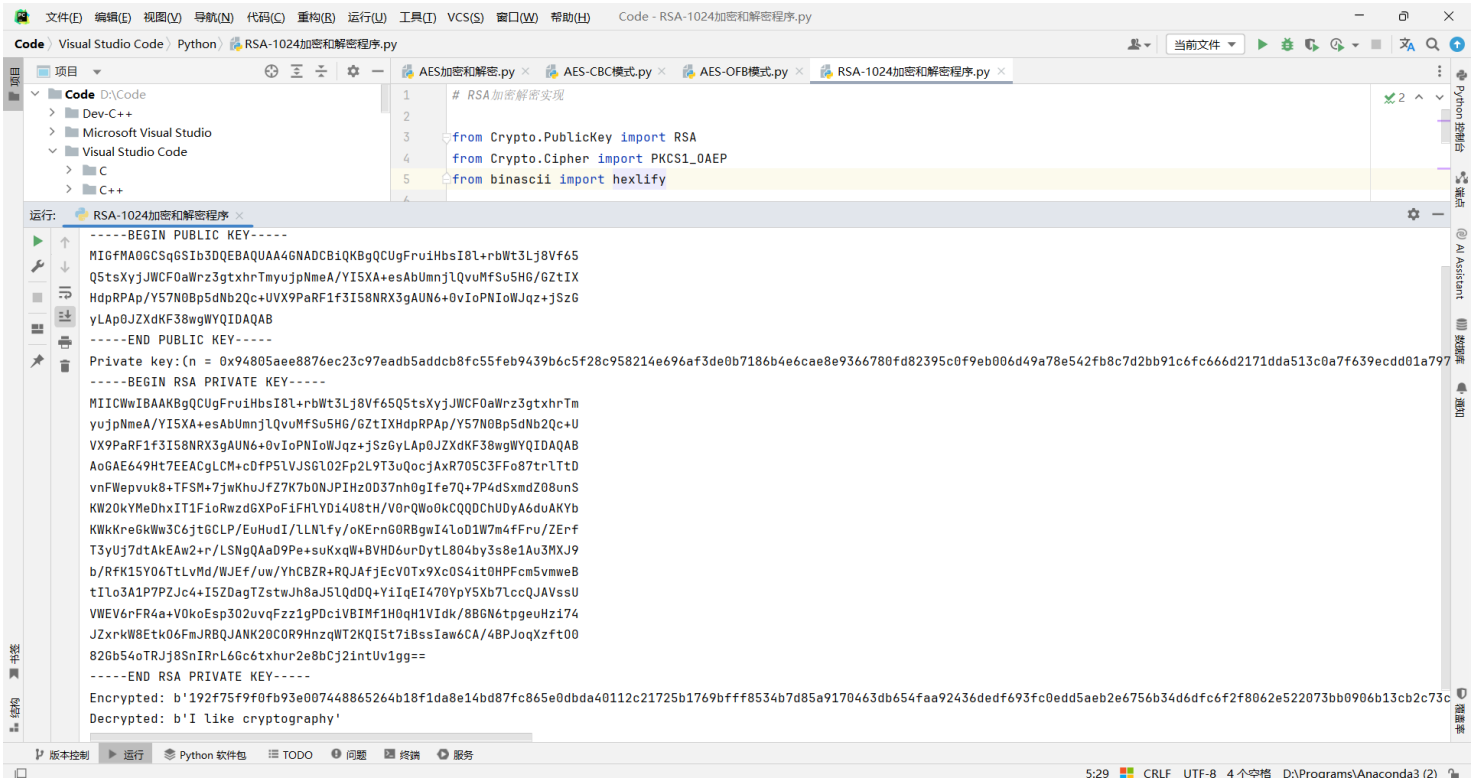

图 2-1 RSA-1024 加密和解密程序

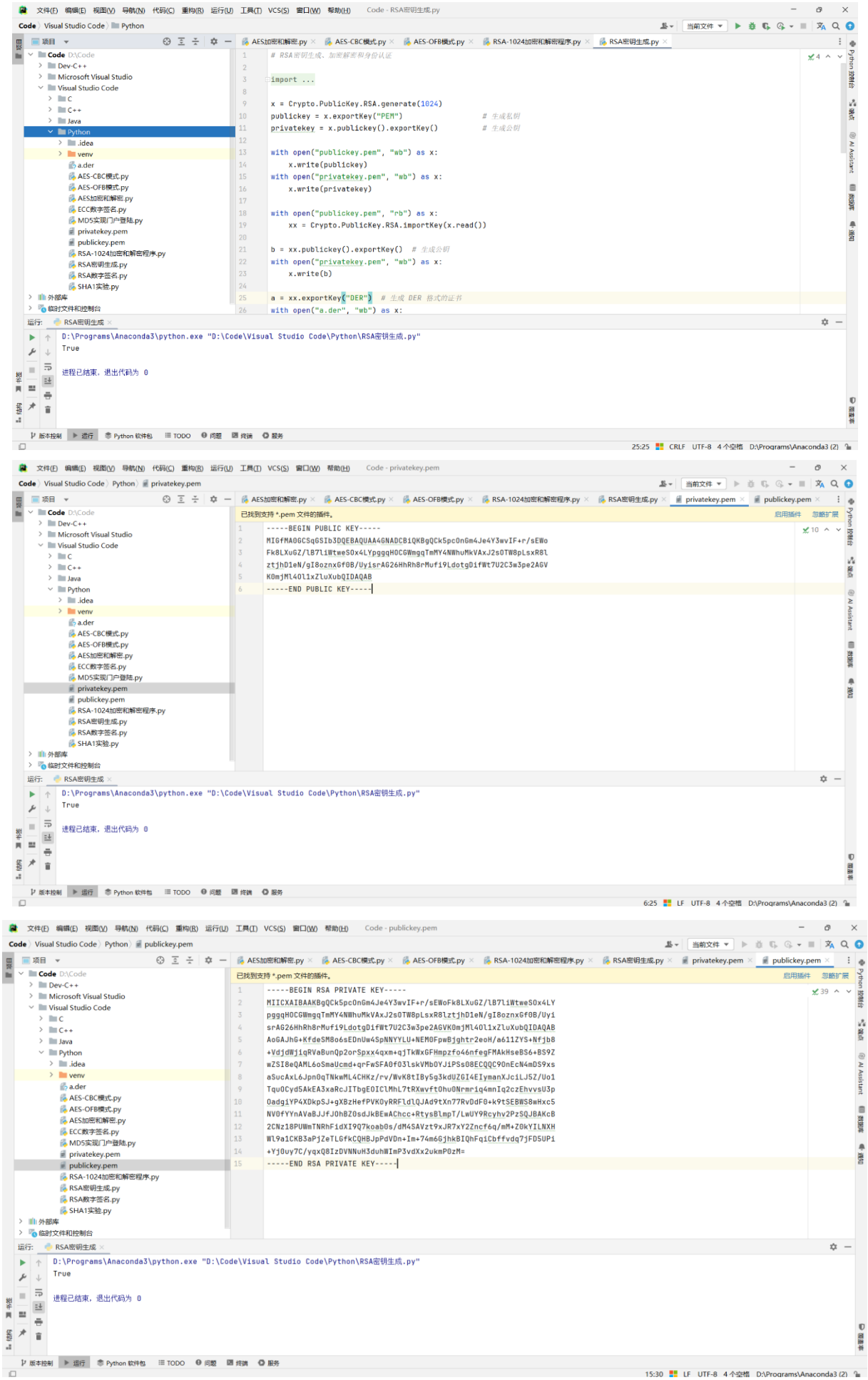
Code - RSA密钥生成.py
AES加密和解密.py
AES-CBC模式.py
AES-OFB模式.py
RSA-1024加密和解密程序.py
RSA密钥生成.py
RSA密钥生成、加密解密和身份认证
import ...
x = Crypto.PublicKey.RSA.generate(1024)
publickey = x.exportKey("PEM") # 生成私钥
privatekey = x.publickey().exportKey() # 生成公钥
with open("publickey.pem", "wb") as x:
x.write(publickey)
with open("privatekey.pem", "wb") as x:
x.write(privatekey)
with open("publickey.pem", "rb") as x:
xx = Crypto.PublicKey.RSA.importKey(x.read())
b = xx.publickey().exportKey() # 生成公钥
with open("privatekey.pem", "wb") as x:
x.write(b)
a = xx.exportKey("DER") # 生成 DER 格式的证书
with open("a.der", "wb") as x:
运行: RSA密钥生成
D:\Programs\Anaconda3\python.exe "D:\Code\Visual Studio Code\Python\RSA密钥生成.py"
True
进程已结束，退出代码为 0
Code - privatekey.pem
privatekey.pem
publickey.pem
已找到支持 *.pem 文件的插件。
启用插件
忽略扩展
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCk5pcOnGm4Je4Y3wvIF+r/sEWo
Fk8LXuGZ/lB7liWtweSOx4LYpggqHOCGWmgqTmMY4NWhuMkVAxJ2sOTW8pLsxR8l
ztjhD1eN/gI8oznxGfOB/UyisrAG26HhRh8rMufi9LdotgDifWt7U2C3w3pe2AGV
KOmjMl4Ol1xZluXubQIDAQAB
-----END PUBLIC KEY-----
publickey.pem
已找到支持 *.pem 文件的插件。
启用插件
忽略扩展
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCk5pcOnGm4Je4Y3wvIF+r/sEWoFk8LXuGZ/lB7liWtweSOx4LY
pggqHOCGWmgqTmMY4NWhuMkVAxJ2sOTW8pLsxR8lztjhD1eN/gI8oznxGfOB/Uyi
srAG26HhRh8rMufi9LdotgDifWt7U2C3w3pe2AGVK0mjMl4Ol1xZluXubQIDAQAB
AoGAJhG+KfdeSM8o6sEDnUw4SpNNYYLU+NEMOFpwBjghtr2eoH/a611ZYS+Nfjb8
+VdjdWjiqRVaBunQp2orSpxx4qxm+qjTkWxGFHmpzfo46nfegFMAkHseBS6+BS9Z
wZSI8eQAML6oSmaUcmd+qrFwSFAOfO3lskVMbOYJiPSsO8ECQQC9OnEcN4mDS9xs
aSucAxL6JpnOqTNkwML4CHKz/rv/WvK8tIBy5g3kdUZGI4EIymanXJc1LJ5Z/Uo1
TquOCyd5AkEA3xaRcJITbgEOIClMhL7tRXwvftOhuONrmriq4mnIq2czEhvysU3p
OadgiYP4XDkpSJ+gXBzHefPVKOyRRFldlQJAd9tXn77RvDdF0+k9tSEBWS8wHxc5
NV0fYYnAVaBJJfJOhBZOsdJkBEwAChcc+RtysBlmpT/LwUY9Rcyhv2PzSQJBAKcB
2CNz18PUWmTNRhFidXI9Q7koab0s/dM4SAVzt9xJR7xY2Zncf6q/mM+Z0kYILNXH
Wl9a1CKB3aPjZeTLGfkCQHBJpPdVDn+Im+74m6GjhkBIQhFqiCbffvdq7jFD5UPi
+YjOuy7C/yqxQ8IzDVNNoH3duhWImP3vdXx2ukmP0zM=
-----END RSA PRIVATE KEY-----
运行: RSA密钥生成
D:\Programs\Anaconda3\python.exe "D:\Code\Visual Studio Code\Python\RSA密钥生成.py"
True
进程已结束，退出代码为 0

图 2-2 RSA 密钥生成

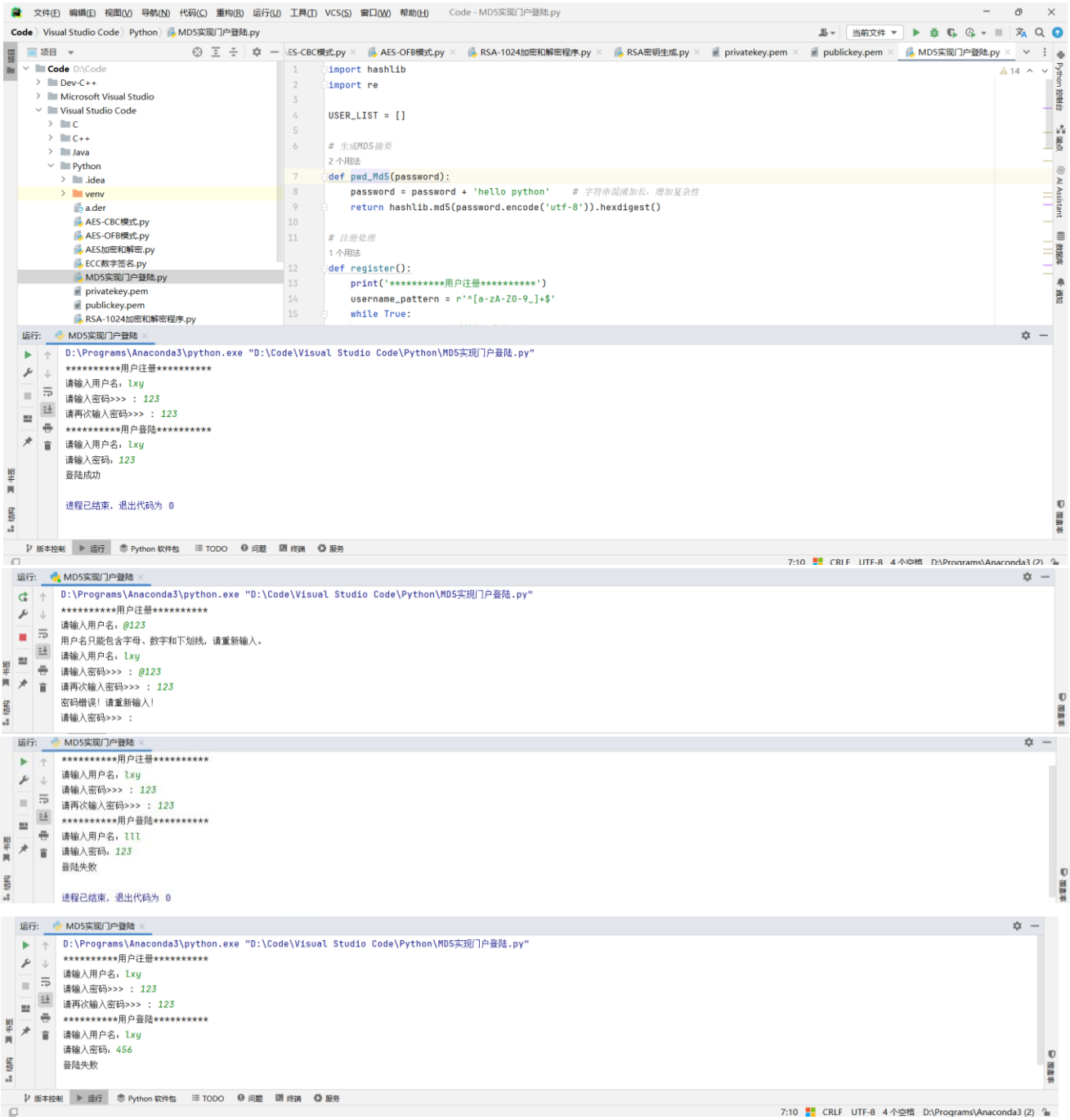

图 3-1 MD5 实现门户登陆

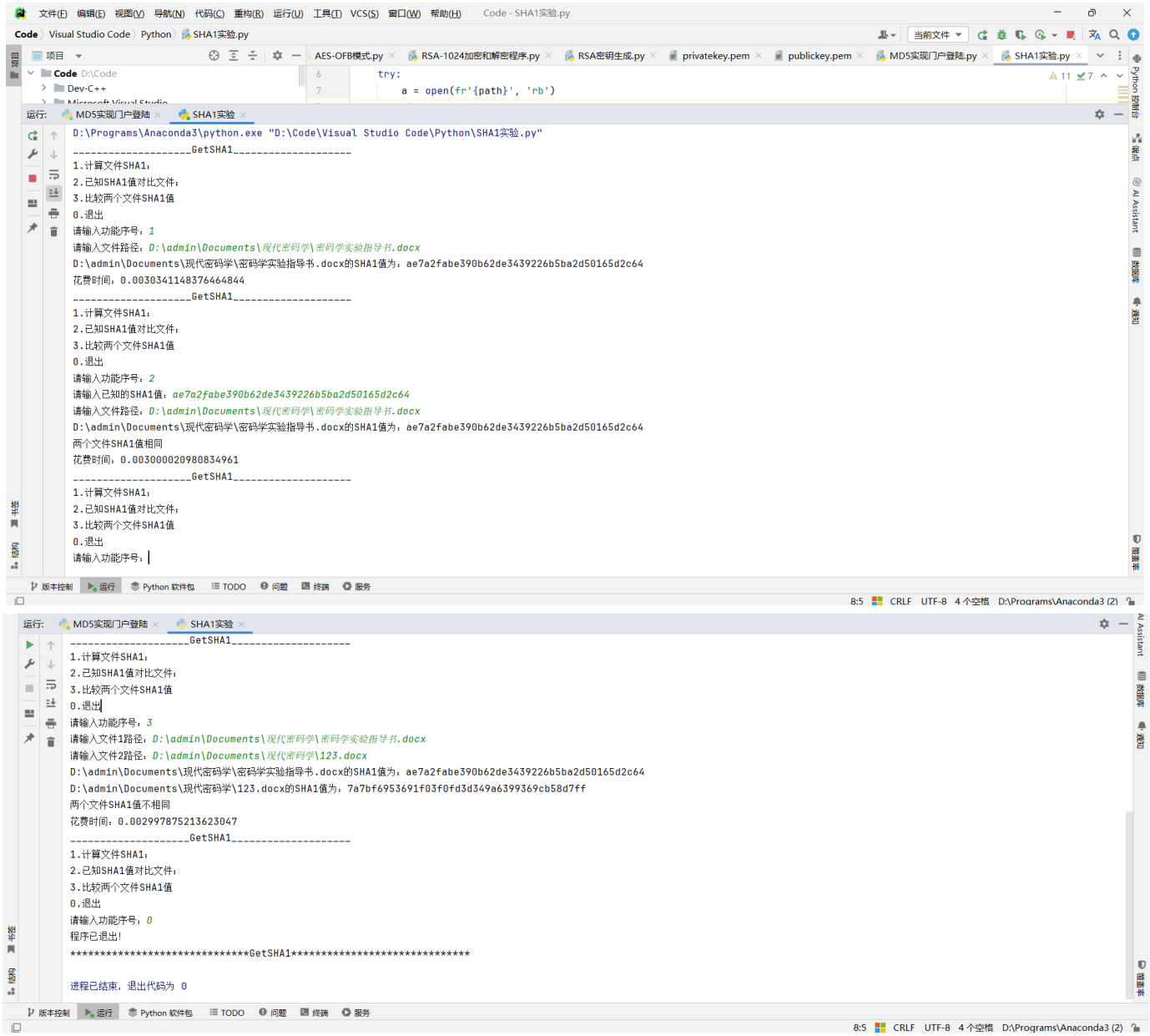
文件(F) 编辑(E) 视图(V) 导航(N) 代码(C) 重构(R) 运行(U) 工具(T) VCS(S) 窗口(W) 帮助(H)
Code - SHA1实验.py
Code 〉 Visual Studio Code 〉 Python 〉 SHA1实验.py
当前文件
项目
Code D:\Code
Dev-C++
AES-OFB模式.py
RSA-1024加密和解密程序.py
RSA密钥生成.py
privatekey.pem
publickey.pem
MD5实现门户登陆.py
SHA1实验.py
try:
a = open(fr'{path}', 'rb')
运行:
MD5实现门户登陆
SHA1实验
D:\Programs\Anaconda3\python.exe "D:\Code\Visual Studio Code\Python\SHA1实验.py"
--------------------GetSHA1--------------------
1.计算文件SHA1；
2.已知SHA1值对比文件；
3.比较两个文件SHA1值
0.退出
请输入功能序号：1
请输入文件路径：D:\admin\Documents\现代密码学\密码学实验指导书.docx
D:\admin\Documents\现代密码学\密码学实验指导书.docx的SHA1值为：ae7a2fabe390b62de3439226b5ba2d50165d2c64
花费时间：0.0030341148376464844
--------------------GetSHA1--------------------
1.计算文件SHA1；
2.已知SHA1值对比文件；
3.比较两个文件SHA1值
0.退出
请输入功能序号：2
请输入已知的SHA1值：ae7a2fabe390b62de3439226b5ba2d50165d2c64
请输入文件路径：D:\admin\Documents\现代密码学\密码学实验指导书.docx
D:\admin\Documents\现代密码学\密码学实验指导书.docx的SHA1值为：ae7a2fabe390b62de3439226b5ba2d50165d2c64
两个文件SHA1值相同
花费时间：0.003000020980834961
--------------------GetSHA1--------------------
1.计算文件SHA1；
2.已知SHA1值对比文件；
3.比较两个文件SHA1值
0.退出
请输入功能序号：
版本控制 运行 Python 软件包 TODO 问题 终端 服务
8:5 CRLF UTF-8 4 个空格 D:\Programs\Anaconda3 (2)
运行:
MD5实现门户登陆
SHA1实验
--------------------GetSHA1--------------------
1.计算文件SHA1；
2.已知SHA1值对比文件；
3.比较两个文件SHA1值
0.退出
请输入功能序号：3
请输入文件1路径：D:\admin\Documents\现代密码学\密码学实验指导书.docx
请输入文件2路径：D:\admin\Documents\现代密码学\123.docx
D:\admin\Documents\现代密码学\密码学实验指导书.docx的SHA1值为：ae7a2fabe390b62de3439226b5ba2d50165d2c64
D:\admin\Documents\现代密码学\123.docx的SHA1值为：7a7bf6953691f03f0fd3d349a6399369cb58d7ff
两个文件SHA1值不相同
花费时间：0.002997875213623047
--------------------GetSHA1--------------------
1.计算文件SHA1；
2.已知SHA1值对比文件；
3.比较两个文件SHA1值
0.退出
请输入功能序号：0
程序已退出!
********************GetSHA1********************
进程已结束，退出代码为 0
版本控制 运行 Python 软件包 TODO 问题 终端 服务
8:5 CRLF UTF-8 4 个空格 D:\Programs\Anaconda3 (2)

图 3-2 SHA1 实验

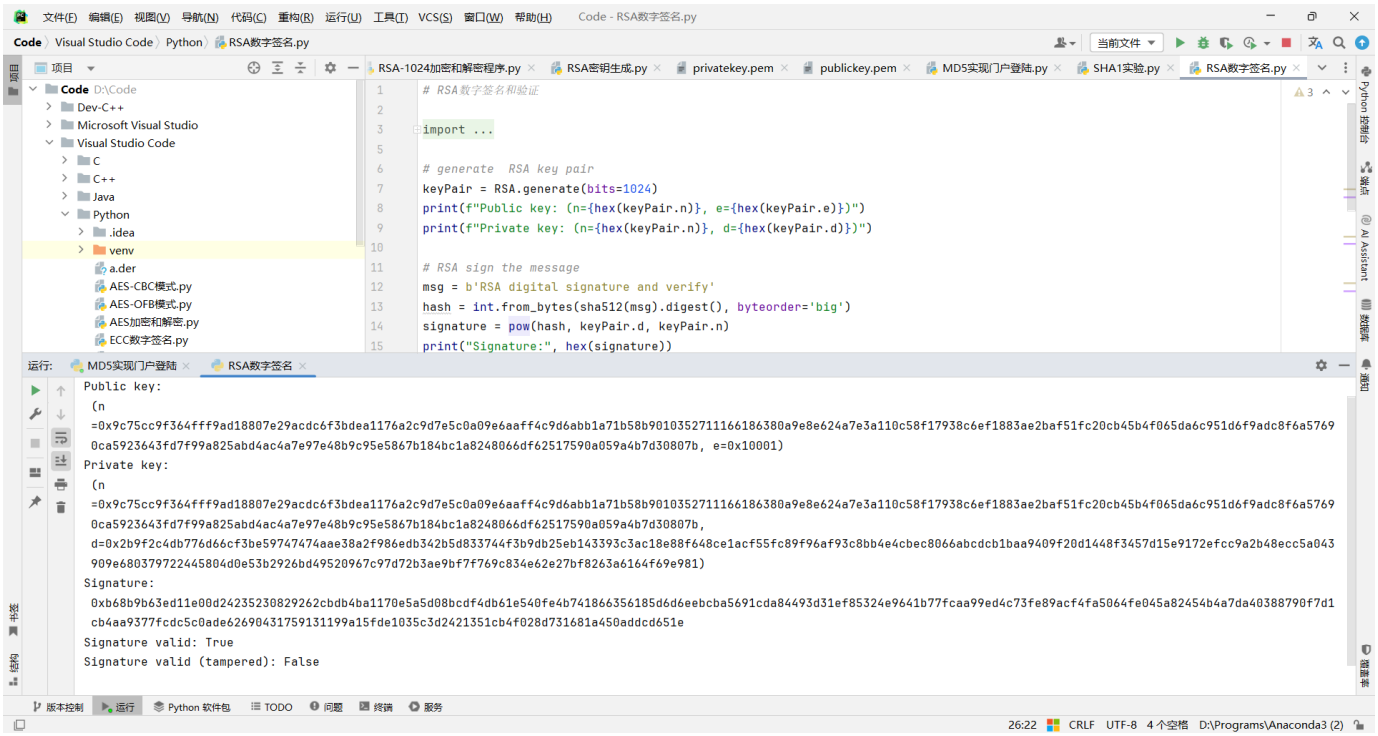

图 4-1 RSA 数字签名

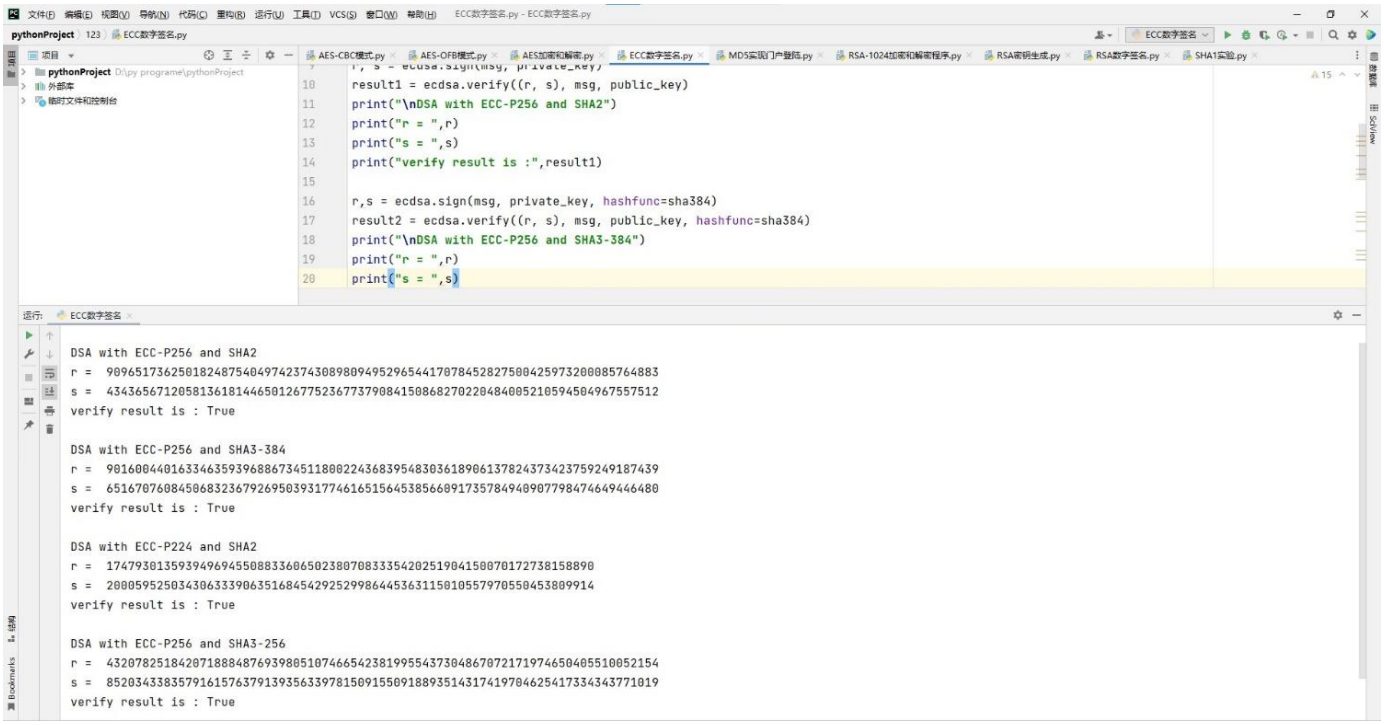

图 4-2 ECC 数字签名