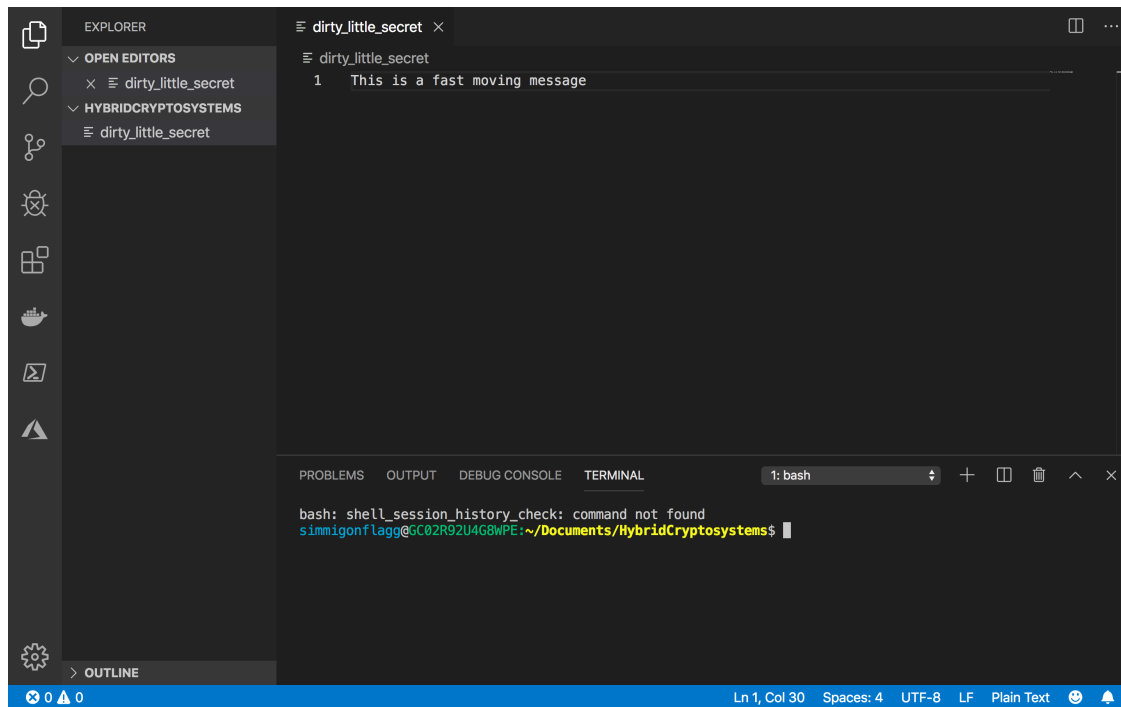
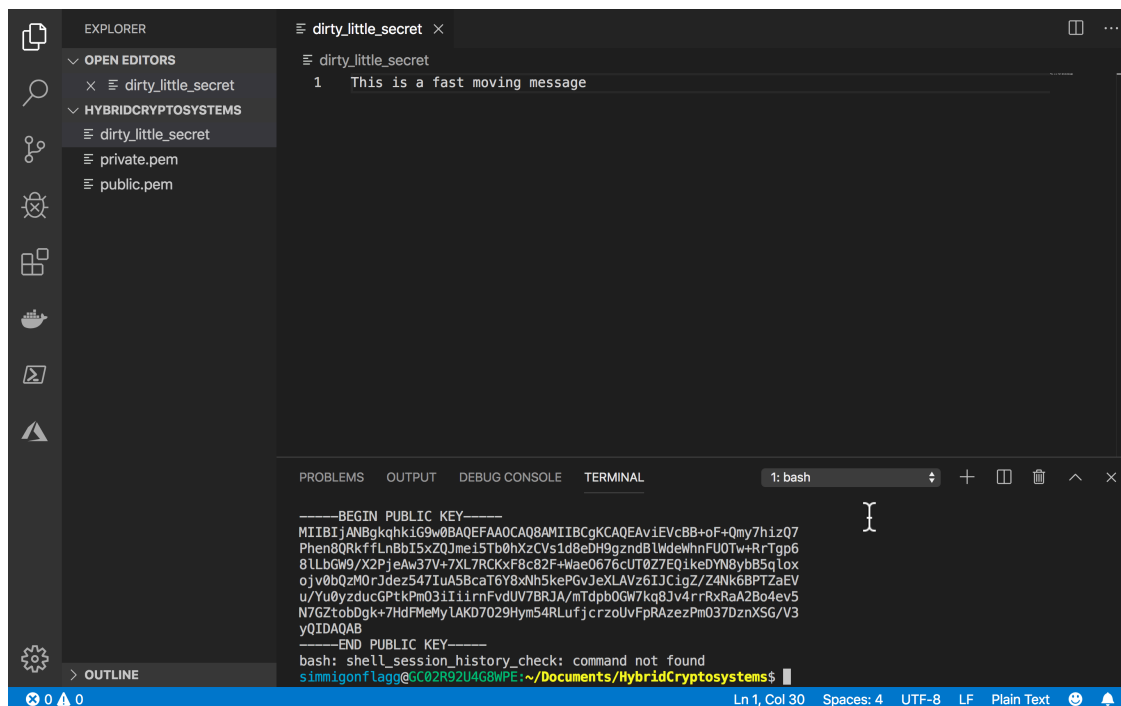


Make a Confession



The screenshot shows the Visual Studio Code interface. The Explorer panel on the left shows a project named 'HYBRIDCRYPTOSYSTEMS' with a file named 'dirty_little_secret'. The Editor panel shows the file 'dirty_little_secret' with the text '1 This is a fast moving message'. The Terminal panel at the bottom shows a bash shell with the prompt 'simmigonflagg@5C02R92U4G8WPE:~/Documents/HybridCryptosystems\$'. The status bar at the bottom indicates 'Ln 1, Col 30', 'Spaces: 4', 'UTF-8', 'LF', 'Plain Text'.

Generate an RSA Keypair



The screenshot shows the Visual Studio Code interface. The Explorer panel on the left shows a project named 'HYBRIDCRYPTOSYSTEMS' with files named 'dirty_little_secret', 'private.pem', and 'public.pem'. The Editor panel shows the file 'dirty_little_secret' with the text '1 This is a fast moving message'. The Terminal panel at the bottom shows a bash shell with the prompt 'simmigonflagg@5C02R92U4G8WPE:~/Documents/HybridCryptosystems\$'. The terminal output shows the command 'openssl genrsa -out private.pem 2048' and the resulting private key. The status bar at the bottom indicates 'Ln 1, Col 30', 'Spaces: 4', 'UTF-8', 'LF', 'Plain Text'.

Trade Public Keys

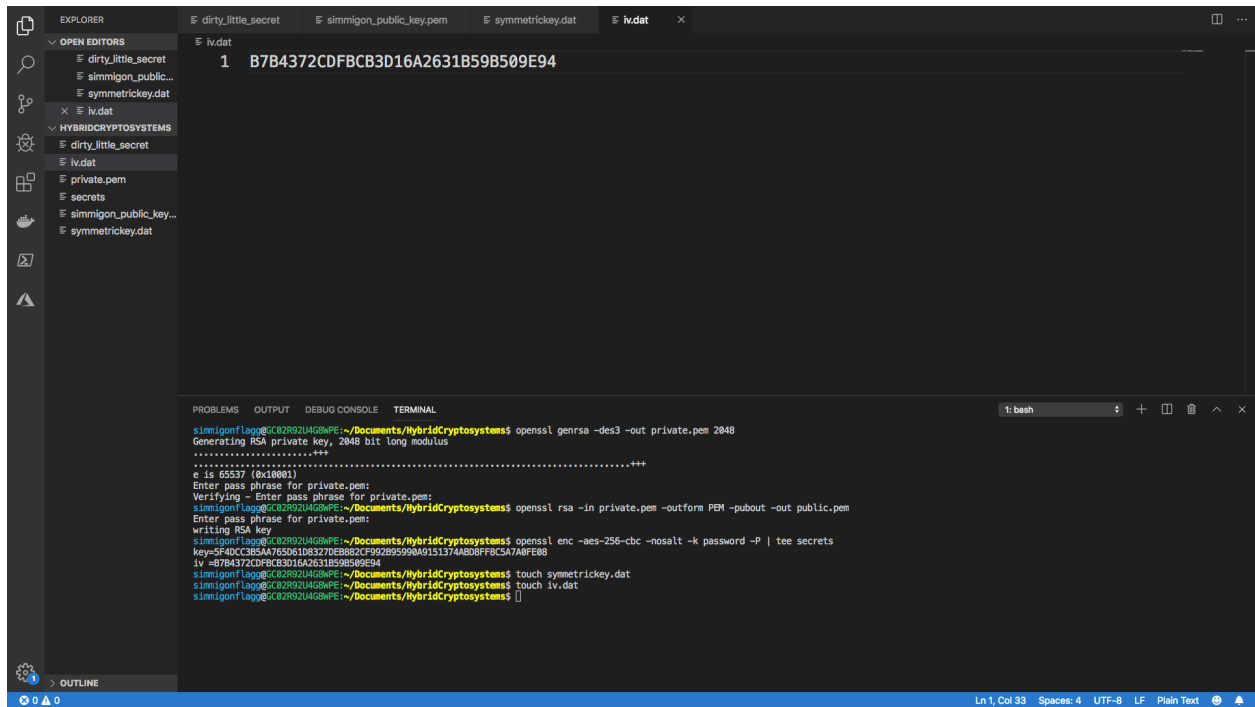
```
dirty_little_secret
1 This is a fast moving message

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAviEvcBB+oF+Qmy7hizQ7
Phen8QRkffLnBb15xZQJmei5Tb0hXzCVs1d8eDH9gznd8lWdeWhnFU0Tw+RrTgp6
8lLbGW9/X2PjeAw37V+7XL7RCKx8F8c2F+Wae0676cUT0Z7EQikeDYN8yb85qloX
ojv0bQzM0rJdez547IuA5BcatY8xNh5kePGvJeXLAVz61JCigZ/Z4Nk68BPTZaEV
u/Yu0yzducGPtkPm03iIiirnfvdUV7BRJA/mTdpb0GW7kq8Jv4rrRxRaA2Bo4ev5
N7GZtobDgk+7HdFMeMyLAKD7029Hym54RLufjcrzoUvFpRAzezPm037DznXSG/V3
yQIDAQAB
-----END PUBLIC KEY-----
bash: shell_session_history_check: command not found
simmigonflagg@GC02R92U4G8WPE:~/Documents/HybridCryptosystems$
```

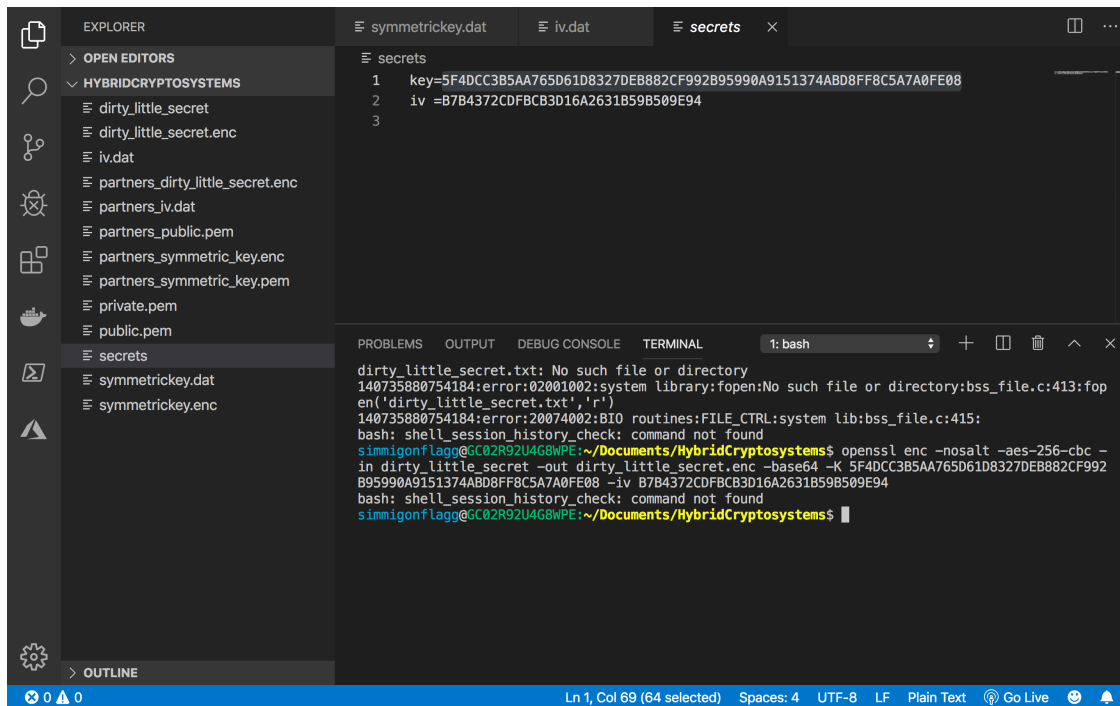
Generate an AES Key

```
dirty_little_secret symmetrickey.dat iv.dat
1 B7B4372CDFBCB3D16A2631B59B509E94

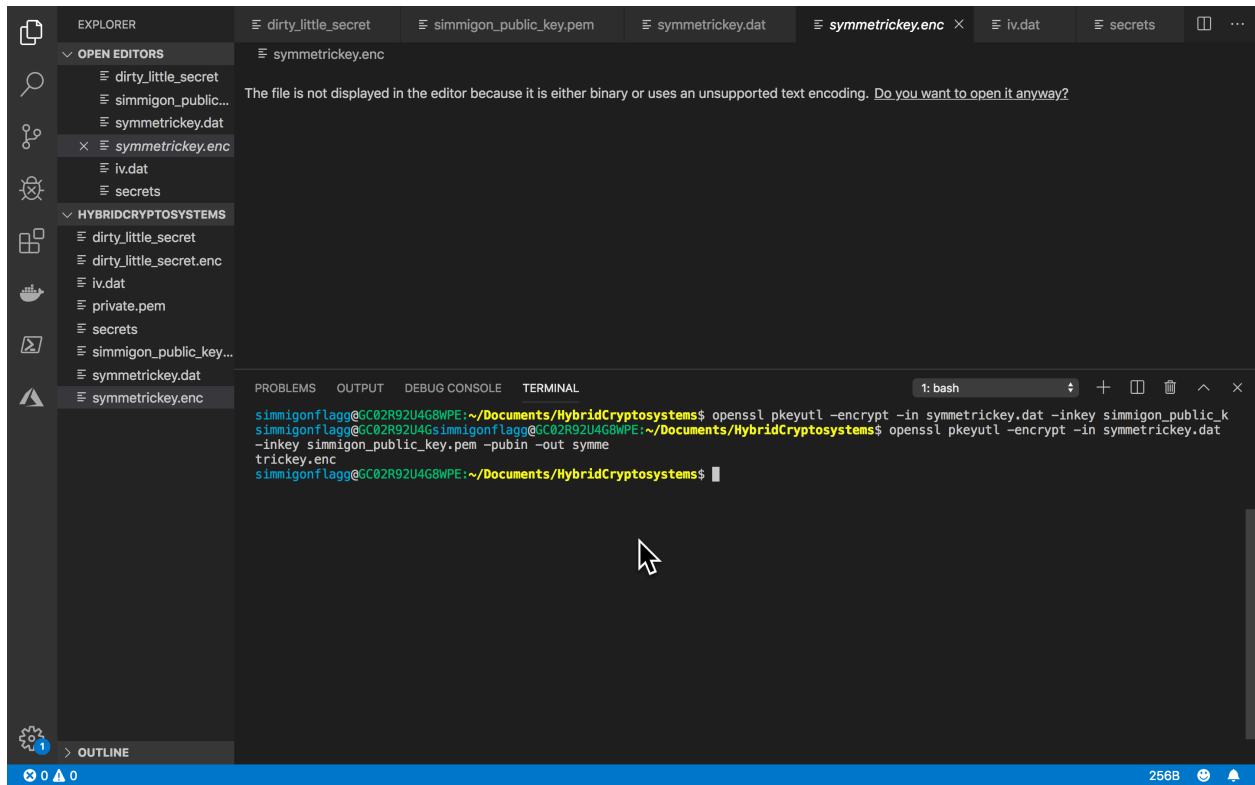
u/Yu0yzducGPtkPm03iIiirnfvdUV7BRJA/mTdpb0GW7kq8Jv4rrRxRaA2Bo4ev5
N7GZtobDgk+7HdFMeMyLAKD7029Hym54RLufjcrzoUvFpRAzezPm037DznXSG/V3
yQIDAQAB
-----END PUBLIC KEY-----
bash: shell_session_history_check: command not found
simmigonflagg@GC02R92U4G8WPE:~/Documents/HybridCryptosystems$ openssl enc -aes-256-cbc -nosalt -k passw
ord -P | tee secrets
key=5F4DCC3B5AA765D61D8327DEB882CF992B95990A9151374ABD8FF8C5A7A0FE08
iv =B7B4372CDFBCB3D16A2631B59B509E94
bash: shell_session_history_check: command not found
simmigonflagg@GC02R92U4G8WPE:~/Documents/HybridCryptosystems$
```



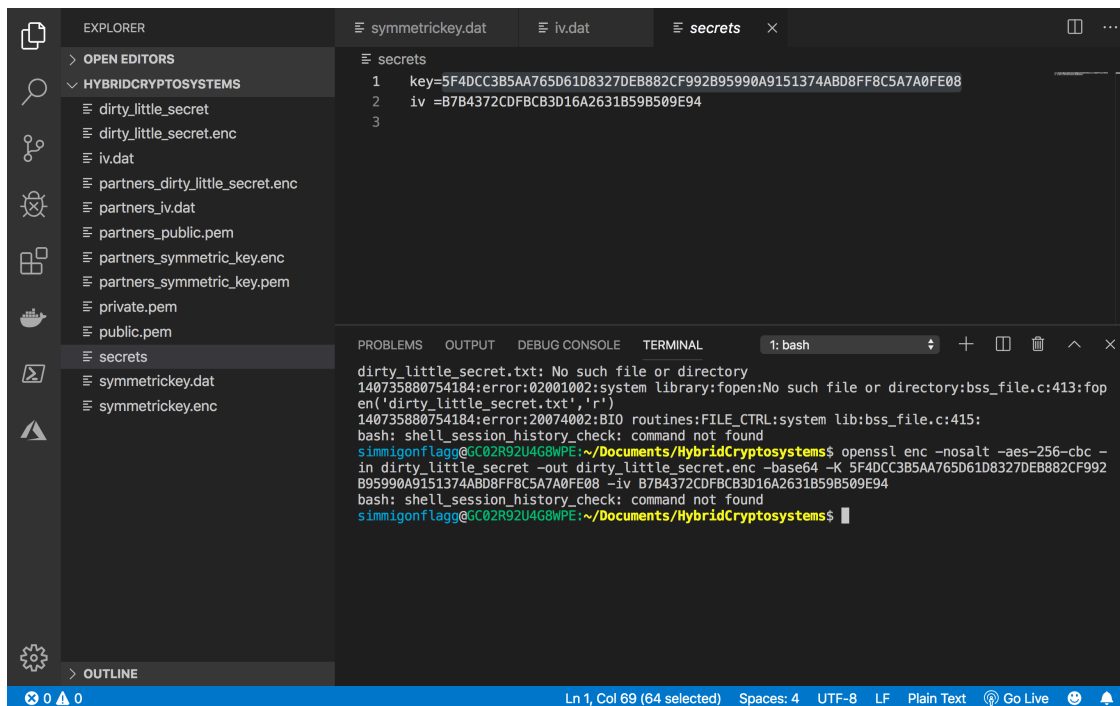
Encrypt Your Message



Encrypt Your Symmetric Key



Trade Files



Decrypt!