Crypto Assignment - The Message Game

Write a Python Script, which behaves as follows -

1. It asks for a message from User
2. It returns back the Encrypted Message to the User and the digital Signature of the encrypted message.
3. It then asks for the signature from User, and the encrypted message.
4. If signature matches, it tries to decrypt the message (which is successful if message is not tampered), and returns error if sign doesn't match or decryption fails, else it returns the decrypted message to user (which should always be same as User gave in step 1, that's actually the Integrity check!!).
5. It asks for User to quit or Continue, continuing goes back to step 1.