University of Utah

Computer Networks

CS 4480

Programming Assignment 3

Author:
John Young
UID:
U1071673

Professors:
Sneha Kasera
H. James de St. Germain

April 20, 2019

Table of Contents

1 Certification

I, John Young, certify that I wrote all submitted code from scratch and did not copy it in part or whole from another source. Any references used in the completion of the assignment are cited in my written work.

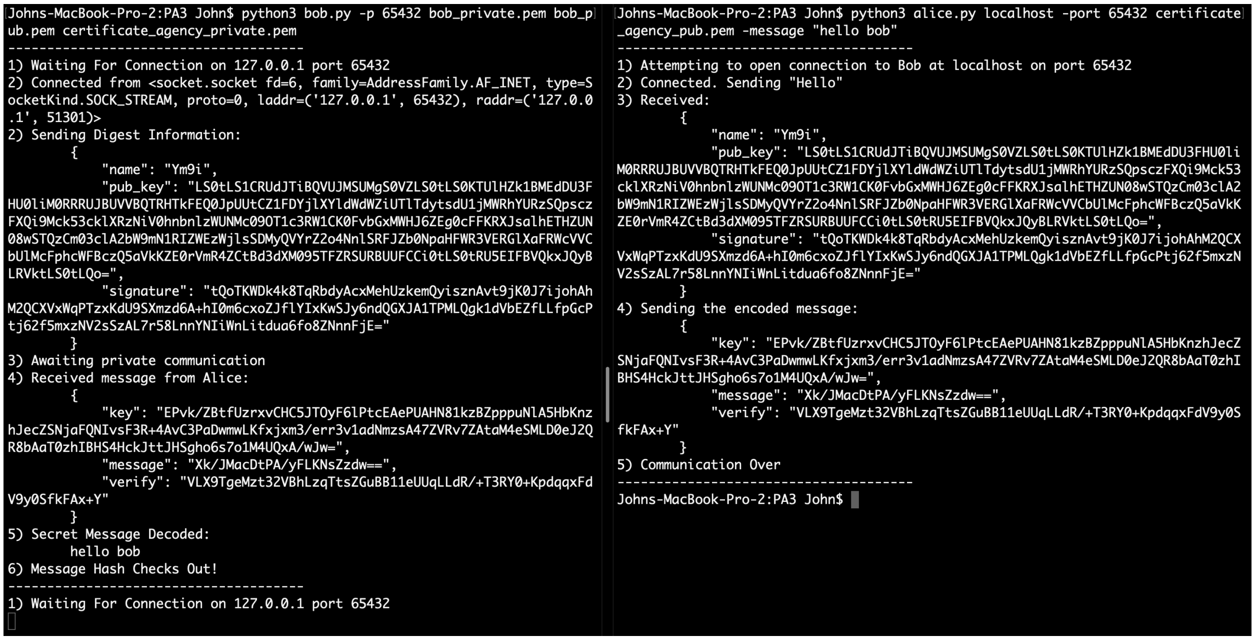
1.1 Citations

I utilized standard API Libraries that are linked in the assignment page. I also utilized the argparse library API.

2 Introduction

`bob.py` acts as Bob and is intended to start first and wait for a connection from Alice. `alice.py` acts as Alice, initializing a connection to Bob and sending a simple message `'Hello'`. When Bob gets a message from Alice he replies with his Digest, which contains his name, his public key and his signature. Alice then receives Bob's digest and verifies the message is from Bob by checking it with a Certificate Agencies public key. Upon good verification, Alice sends her encoded message to Bob, which contains her symmetric key (Encrypted with Bob's public key so no one can read it but Bob), the message and verification, both encrypted with the symmetric key. Bob then receives the message from Alice and verifies it's integrity via decryption it and comparing hash values. This entire process can be seen inf Figure 1.

There are more details that can be seen in my code documentation that explain this process more in depth. From dong this assignment I understand the details of a secure communication using RSA and hashing. I understand that the connection should use hashing, RSA, a 3rd party certificate agency and a transfer of an encrypted key in order to securely set up a connection between two or more parties. If done correctly the parties can use the symmetric key in addition to a initialization vector to communicate securely.



```
Johns-MacBook-Pro-2:PA3 John$ python3 bob.py -p 65432 bob_private.pem bob_p
ub.pem certificate_agency_private.pem
--------------------------------------
1) Waiting For Connection on 127.0.0.1 port 65432
2) Connected from <socket.socket fd=6, family=AddressFamily.AF_INET, type=S
ocketKind.SOCK_STREAM, proto=0, laddr=('127.0.0.1', 65432), raddr=('127.0.0
.1', 51301)>
2) Sending Digest Information:
        {
            "name": "Ym9i",
            "pub_key": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlHZk1BMEdDU3F
HU0liM0RRRUJBUVVBQTRHTkFEQ0JpUUtCZ1FDYjlXYldWdWZiUTlTdytsdU1jMWRhYURzSQpscz
FXQi9Mck53cklXRzNiV0hnbnlzWUNMc090T1c3RW1CK0FvbGxMWHJ6ZEg0cFFKRXJsalhETHZUN
08wSTQzCm03clA2bW9mN1RIZWEzWjlsSDMyQVYrZ2o4NnlSRFJZb0NpaHFWR3VERGlXaFRWcVVC
bUlMcFphcWFBczQ5aVkKZE0rVmR4ZCtBd3dXM095TFZRSURBUUFCCi0tLS0tRU5EIFBVQkxJQyB
LRVktLS0tLQo=",
            "signature": "tQoTKWDk4k8TqRbdyAcxMehUzkemQyisznAvt9jK0J7ijohAh
M2QCXVxWqPTzxKdU9SXmzd6A+hI0m6cxoZJflYIxKwSJy6ndQGXJA1TPMLQgk1dVbEZfLLfpGcP
tj62f5mxzNV2sSzAL7r58LnnYNIiWnLitdua6fo8ZNnnFjE="
        }
3) Awaiting private communication
4) Received message from Alice:
        {
            "key": "EPvk/ZBtfUzrxvCHC5JTOyF6lPtcEAePUAHN81kzBZpppuNlA5HbKnz
hJecZSNjaFQNIvsF3R+4AvC3PaDwmwLKfxjxm3/err3v1adNmzsA47ZVRv7ZAtaM4eSMLD0eJ2Q
R8bAaT0zhIBHS4HckJttJHSgho6s7o1M4UQxA/wJw=",
            "message": "Xk/JMacDtPA/yFLKNsZzdw==",
            "verify": "VLX9TgeMzt32VBhLzqTtsZGuBB11eUUqLLdR/+T3RY0+KpdqqxFd
V9y0SfkFAx+Y"
        }
5) Secret Message Decoded:
        hello bob
6) Message Hash Checks Out!
--------------------------------------
1) Waiting For Connection on 127.0.0.1 port 65432
```

```
Johns-MacBook-Pro-2:PA3 John$ python3 alice.py localhost -port 65432 certificate
_agency_pub.pem -message "hello bob"
--------------------------------------
1) Attempting to open connection to Bob at localhost on port 65432
2) Connected. Sending "Hello"
3) Received:
        {
            "name": "Ym9i",
            "pub_key": "LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUlHZk1BMEdDU3FHU0li
M0RRRUJBUVVBQTRHTkFEQ0JpUUtCZ1FDYjlXYldWdWZiUTlTdytsdU1jMWRhYURzSQpsczFXQi9Mck53
cklXRzNiV0hnbnlzWUNMc090T1c3RW1CK0FvbGxMWHJ6ZEg0cFFKRXJsalhETHZUN08wSTQzCm03clA2
bW9mN1RIZWEzWjlsSDMyQVYrZ2o4NnlSRFJZb0NpaHFWR3VERGlXaFRWcVVCbUlMcFphcWFBczQ5aVkK
ZE0rVmR4ZCtBd3dXM095TFZRSURBUUFCCi0tLS0tRU5EIFBVQkxJQyBLRVktLS0tLQo=",
            "signature": "tQoTKWDk4k8TqRbdyAcxMehUzkemQyisznAvt9jK0J7ijohAhM2QCX
VxWqPTzxKdU9SXmzd6A+hI0m6cxoZJflYIxKwSJy6ndQGXJA1TPMLQgk1dVbEZfLLfpGcPtj62f5mxzN
V2sSzAL7r58LnnYNIiWnLitdua6fo8ZNnnFjE="
        }
4) Sending the encoded message:
        {
            "key": "EPvk/ZBtfUzrxvCHC5JTOyF6lPtcEAePUAHN81kzBZpppuNlA5HbKnzhJecZ
SNjaFQNIvsF3R+4AvC3PaDwmwLKfxjxm3/err3v1adNmzsA47ZVRv7ZAtaM4eSMLD0eJ2QR8bAaT0zhI
BHS4HckJttJHSgho6s7o1M4UQxA/wJw=",
            "message": "Xk/JMacDtPA/yFLKNsZzdw==",
            "verify": "VLX9TgeMzt32VBhLzqTtsZGuBB11eUUqLLdR/+T3RY0+KpdqqxFdV9y0S
fkFAx+Y"
        }
5) Communication Over
--------------------------------------
Johns-MacBook-Pro-2:PA3 John$
```

Figure 1: Screen shot of Alice sending a message to Bob. (Bob on the left and Alice on the Right

3 Program Software Engineering

I did my best to ensure good software programming. I used consistent methods between both `alice.py` and `bob.py` in order manipulate the data using encryption, decryption, encode or decode. I also used comments on every method explaining what each parameter is, what it is meant to do and what it should return. In addition to my code documentation, I also used types when initializing any new variable to help show how I intended on using that object.

4 Errors or Extensions

I'm unaware of any errors and wrote this program with the intention on not having any errors. However I made some assumptions where the assignment was not clear. I assume that `alice.py` exits after finishing the steps shown in Figure 1. I assume that `bob.py` can either exit after finishing the steps shown in Figure 1 or repeat the process. I programming `bob.py` to repeat the process after finishing. I also assume that `bob.py` only needs to support one connection at a time so that is how I implemented it.