Daniel Ornelas

Spring 2018

Computer Security

Assignment 2

**Introduction**

In this assignment, we created a cryptographic protocol with key exchange, digital signatures, and encryption. We used the protocol to communicate with a server to test its functionality.

**Part 1**

**Encrypted Keys:**

**DanielPrivateSignClient.pem**

-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAI4ANVyBloDbv3k8

Y1Tho74yqw0g/d1nO4b+QsOVxqFL1+Ddtt9DiWRRbISuRiDMh+VgUG1lhopoBuTL

7BGINamEJPaNVmF2Gh3jvEzD9q26v84nPL4kcYzrcRl8AN+yrTPWJ0Ehs3ZCQHI5

5ldHsH0FJB7y78hD1zXkHNe54ZCZAgMBAAECgYAPclRbqLkPcVgFvxzrCdR/BxH2

TqVu5SDjkVr/3ZYKy65DBrsy1Czo3baZRD/ap4UM3YpCLC4TdjdxwgD+8zsq+Prs

xDbteZ8KhoI2WR+o7+B5DaCdWI0ryC8n59Y/IvrrPFdQRgC4UI9DKpUHWtzqWSgq

BjqQ9NZBI/5/6pwnFQJBAL7SE+q3zrCgTuiGdmrFt5q8BMWnNhBQS81s/O52fJXF

fAea1WrbNwEmaHQDJrelnN7uAKDnv9Za+lZ9MEILmD8CQQC+gS6URDxaX+mSE4NG

/BmoBqBC0kqqyc1nT1bMcuc3Z4x0XBB0184FZi0vfaOxZJIB2jgW5yINfb3cR1sD

MuEnAkEAjkNZDfkTY6NgsQLubhQSGo5qkGFlcSwsF29V8wLrR04Adjr9OblNfNIB

tdxTlT8ngRy34z5kS49wa+LRg6vZSQJAVNRzaGRmN5wkBv8XYwGZbx/cN0UrKJgK

FinXLd0wppQ+kAX68fyy6eaQ0mfw/2oYNij09wXfPQC0DaXcmjUK2wJAdyq2xiMa

1Vr8NzXWB5oiONQweeypbxZ+EsvNUGhsTMbrCoCwOZylQa2rFfPhzbtRtcsjXN1r

waTzQcevRBrwqA==

-----END PRIVATE KEY-----

**DanielPublicSignClient.pem**

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCOADVcgZaA2795PGNU4aO+MqsN

IP3dZzuG/kLDlcahS9fg3bbfQ4lkUWyErkYgzIflYFBtZYaKaAbky+wRiDWphCT2

jVZhdhod47xMw/atur/OJzy+JHGM63EZfADfsq0z1idBIbN2QkByOeZXR7B9BSQe

8u/IQ9c15BzXueGQmQIDAQAB

-----END PUBLIC KEY-----

**DanielServerPrivate.pem**

-----BEGIN PRIVATE KEY-----

MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAJCAXnKOsgAB/Mlk

pM8P1ISNgmOL4F5GQ54Wfk4PWAGaIl2VUr8dJCENWQYKbfeVr3ZJIH/WvXoLZJu1

GcG+1zuoFF7qG7cxupoGKz84emmYFLXHY6xuSTsL6Ck8E/k0tfjZbSuK8Yyjk0n9

YxO5Pv+bo1hcTunbY2Y1gOpDt5ddAgMBAAECgYBY2RU5itOXfaFYkzFiv3EEL55E

ZvUGAl4BDgOLK5QJKCSJNg8yw1A7omFifXcwDDFeoYgCEp9eMzMhKjE0F4tuiFqG

ZnqMTJOBhUOXwh4M4DG+edxkdF7PinE1EVQNhk0f0xTiF835cXu0idwdzs5YKgEU

4qbSaqHszbuwfC5DYQJBAPDaveIG9FH+0dajQHNGVYj9YLB6zuUcCtFOb4K3xNmQ

n39OCC77FgEyu9f0SVU9D+uHiPLyxN6cbIqpbkuatusCQQCZlosEuH+JsJzg+c8P

rKOYyCg9anoek/r1HpUQXRNoPdupyJpb6VfJoZ9XFWS5aonVqNqErf1V5REMa6Wy

SejXAkB4o3fckNMrhtEgCyErHB2XwiH+A2VCCKu6bukXtmhY+UGKiFE9BvLcosbH

wkpA8ZbZyEdmOQc24W7UfU0LfXEFAkA7yvnwKousZQ+OHnLYHVPLZREVZ+CHCwFG

cFOD/VhS2tIrtScy5RMCMmPAGVoPPUTP416/DKV1zSnn9fiaAmAdAkBpAdkBmFHh

O8ZS38p3wP3Dtei0nLwLeWruxgwofFMPSM9N3BKtZBWmMH50x0hABdTLGJthM/vK

yYSltvsWrK3Y

-----END PRIVATE KEY-----

**DanielServerPublic.pem**

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCQgF5yjrIAAfzJZKTPD9SEjYJj

i+BeRkOeFn5OD1gBmiJdlVK/HSQhDVkGCm33la92SSB/1r16C2SbtRnBvtc7qBRe

6hu3MbqaBis/OHppmBS1x2Osbkk7C+gpPBP5NLX42W0rivGMo5NJ/WMTuT7/m6NY

XE7p22NmNYDqQ7eXXQIDAQAB

-----END PUBLIC KEY-----

**PrivateKeySign2.pem**

-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAJmjXCNOz31ZQEGW

ZBDmrvTBQ2AyARfdn3FfGU6MCoizCladdjh/tDZz9VFuO+t9dzm06R2lLHhFdMUk

tzIf5RSj10DzbEZYDL3j/P/okvaEzhEcsZmZJthWToWFEewKk1HE4uUUyn5qo2Iu

dz7+WzyqmdfI2rbAylzjiqF1Hk/JAgMBAAECgYB9rhfSPkcXyCn7PTZQaRTX3Tzr

dRxV1JL4oA3IpmB7oNKlNhwebcETBlq4qU9U/YbJaweDm7m8DT1PhBBkbZjrunoE

7FBK5jbwZroLKgQWUae9skHskSosgszPJZN1lauZHP422/GW49BhqyeuVPULRdwL

DuJfxJoylDqba85g7QJBANp5xjW1tnsRlIIa8hhh0EV5W+1wPpmQbRd1i+pjcfLZ

+Rt0fcp25RDG0pGQSqsJAvmXUGaYECcwF7UXVL5ZpZsCQQC0BrkKbLpNXpsTQ1Qv

J2u8h60IjzNcClAoAHOLjQ9KkZ5C7mu/42rfZt2mg0pGYjADQCcEX9BwnOyiTc6T

n8hrAkAYcFTGv0vpWl8VarQ4HADzNI8e8VZfUTOS0zhSgMtHUjC2bIKBumkHRmZZ

mB1yInDtwIpi35G3AH82Z6S4IkkPAkAdLZHELMctTw4XWyxD0EHX9q2G257ZZhqD

wT74+U3nKh7afkYcfcGOn9+A43qgWb2qaTVpshXYiraXv8ChkJ4tAkEAwjqfUyk2

WcDhjyQSSqlEbOLgWle7SWXG60e7ubNAfpS9TH5ov0jNwohQ0aMER4KRwyD02mQ1

Nmraow1IuB4Jlg==

-----END PRIVATE KEY-----

**PublicKeySign2.pem**

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZo1wjTs99WUBBlmQQ5q70wUNg

MgEX3Z9xXxlOjAqIswpWnXY4f7Q2c/VRbjvrfXc5tOkdpSx4RXTFJLcyH+UUo9dA

82xGWAy94/z/6JL2hM4RHLGZmSbYVk6FhRHsCpNRxOLlFMp+aqNiLnc+/ls8qpnX

yNq2wMpc44qhdR5PyQIDAQAB

-----END PUBLIC KEY-----

**DanielServerPrivateKey2.pem**

-----BEGIN PRIVATE KEY-----

MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAKozUBi2L7qsZUnU

FC7+O31FTOFU+De0z8uPfmmUYDcem31CH15AYAF0GQ27819hPVX9pK9UELtfqFu4

G07FpfqpmJy4YojjaLZJRFmN+l2ZXPxEhvF2ZY2Vrwi0KQwQIBAOfok8++xDWfCX

EDs0SBiPNyJQuI5hKX0kTiMoGfDPAgMBAAECgYAXcM29OYpFSW0ByAWnmzgSPrMh

7ZPqCCr+PBsK63Z84OhFThAH6RHP4W955sLUBg5ug2plA0zyoXAMgcSxCqObMoej

IL1JsPWasMHfrXpYss48yFqQIvcGEOmApDC5OvFPBQvi+CriovqKBnjluc87FHon

acPZ8eUyd9Nf4PmLcQJBAOHPDxEVGzCK9Fv/Jg/hIV2CSxl/r96CX4jlNoX5lz/J

t/+2swTZJE1L4A28pKycvMUqy4UJtyyeO6Uj3lBVgSsCQQDA9Oak9wYrJKx5eoKk

caoiW7JJKvqkya5dH4uRBLO7OGTsm0Afk/s+kqjB9/izbxdjHTCCMC6Rp3AYf07f

jhTtAkB8rQ+blfS6O66p8Nm6IMqET8FZZdfb2k4XTr9o/6MUFDNknCKBxca2avNd

gk/GApBzqKpQXUnm98Lk7kX8QwmbAkA1a5fvU/SBPUYC28gPfuh7WqehWiTKOovr

fDBHleWsj5BhcRnvpCiKyk+uY9iW1MrExfAIGw7JhHGkVpqfidaBAkEAxkLYD4rV

lIzbsYHp2Li85TxHK/e3Q+2h+gkQG3Ltw5wG7lSB6KgbIzOWSYo4KRIqODcRGDQi

Mw/ttA7lySrk2Q==

-----END PRIVATE KEY-----

**DanielPublicServer2.pem**

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqM1AYti+6rGVJ1BQu/jt9RUzh

VPg3tM/Lj35plGA3Hpt9Qh9eQGABdBkNu/NfYT1V/aSvVBC7X6hbuBtOxaX6qZic

uGKI42i2SURZjfpdmVz8RIbxdmWNla8ItCkMECAQDn6JPPvsQ1nwlxA7NEgYjzci

ULiOYSl9JE4jKBnwzwIDAQAB

-----END PUBLIC KEY-----

**Encryption of Name and Date:**

The plaintext is: Daniel Ornelas, 3/24/2018

The encrypted string is: C1G+0DC+qG4KLkZCpm/NCHHjnoAB98lQkhFMj7fHgwwU0f4gwMNxbJPV3xCktBoebbGbpsZ18PhAVH/mXR71iVi1vpEUNhMCsWibV2brIM0/dSYqAA/0f9CTzpZnuO7FQNLHFdurCYhFWgjAktXbJOr+clI0GmdOOaAwC7nw5Js=

**Base64 Encoding Question:**

If we encode a byte array of length n with Base64, the length of the string would be 4\*(n/3)

Reference : http://www.siddharthpandey.net/how-to-calculate-the-size-of-a-base64-encoded-string/

**Part 2**

-----BEGIN INFORMATION-----

Date: 20-Mar-18

Name: Daniel Ornelas

Username: dornelas4

-----END INFORMATION-----

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCQgF5yjrIAAfzJZKTPD9SEjYJj

i+BeRkOeFn5OD1gBmiJdlVK/HSQhDVkGCm33la92SSB/1r16C2SbtRnBvtc7qBRe

6hu3MbqaBis/OHppmBS1x2Osbkk7C+gpPBP5NLX42W0rivGMo5NJ/WMTuT7/m6NY

XE7p22NmNYDqQ7eXXQIDAQAB

-----END PUBLIC KEY-----

-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCOADVcgZaA2795PGNU4aO+MqsN

IP3dZzuG/kLDlcahS9fg3bbfQ4lkUWyErkYgzIflYFBtZYaKaAbky+wRiDWphCT2

jVZhdhod47xMw/atur/OJzy+JHGM63EZfADfsq0z1idBIbN2QkByOeZXR7B9BSQe

8u/IQ9c15BzXueGQmQIDAQAB

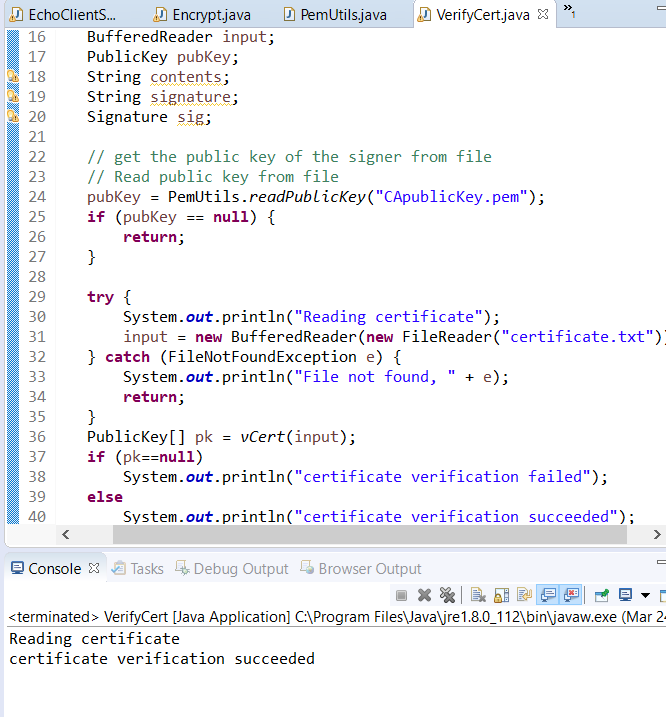
-----END PUBLIC KEY-----

-----BEGIN SIGNATURE-----

kqq52xeq5+m6hy8wuS8V84dBOUJJQvMv/gsi9l2dLiuugcUXZTHFLuxsEstLqRNKyyMAPC/whrHcWxrgTJ+Hq2JAkigNoZOKknIXvms3wSs8c5gDb6+ByflJz/eX9FxP7DcZzS2hrYOfNZvmZnhQ6jskmEXyqkQyKxVCUz+aXtw=

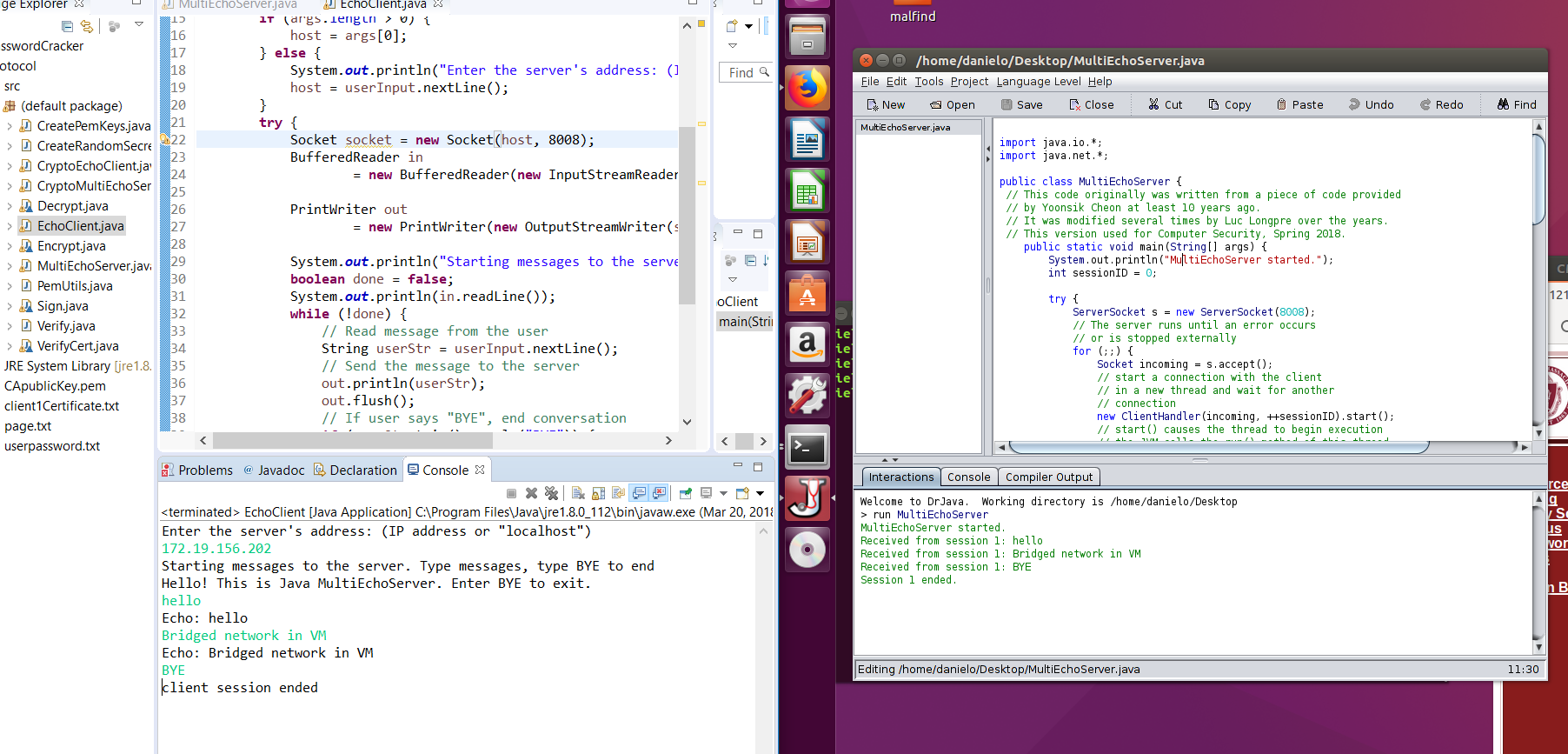
-----END SIGNATURE-----

**Part 3**

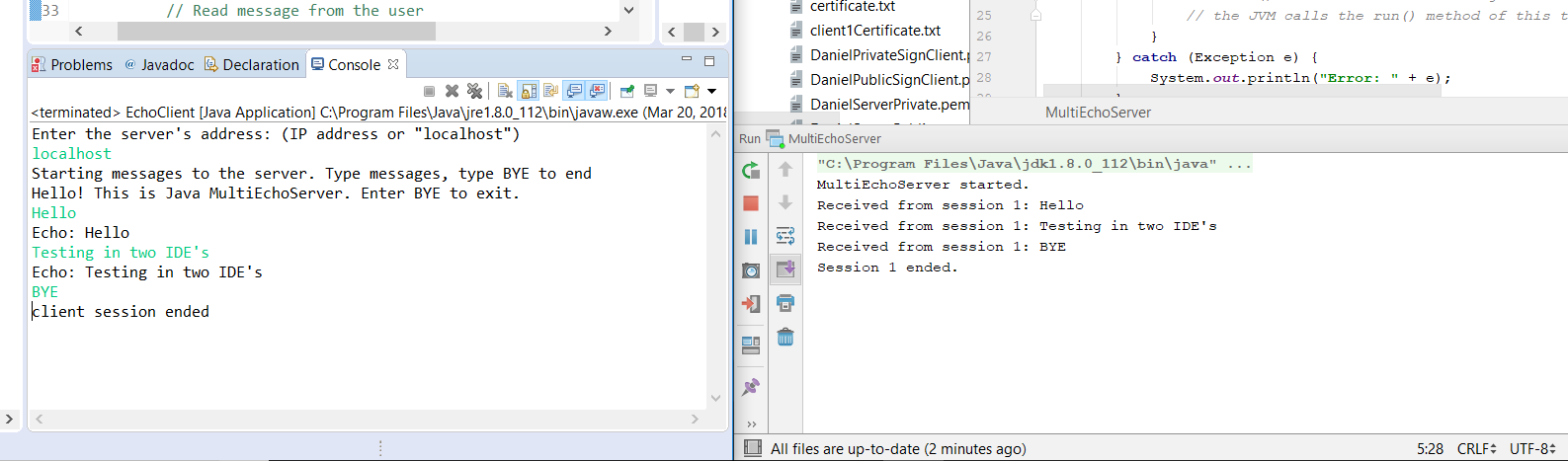
****

**Part 4**

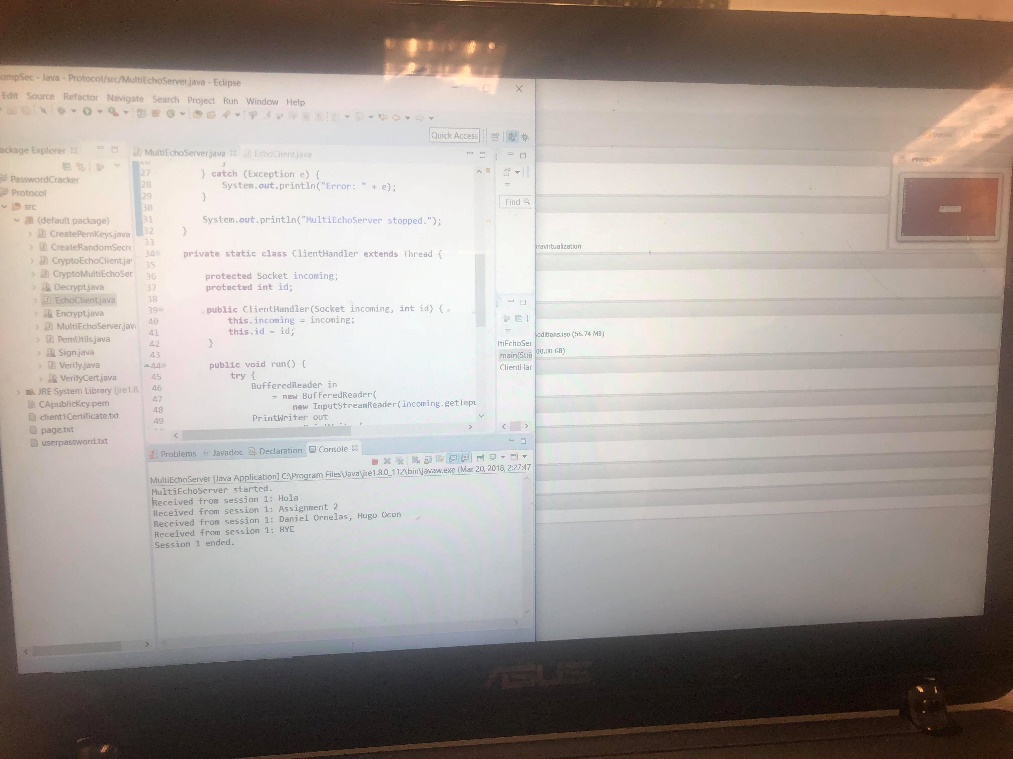
**\*\* For Part 4, I collaborated with Hugo Ocon to test communication from machine to machine, the only contribution between us was to provide the IP address to the other and one person ran the server, the other ran the client, and communication between two machines was tested\*\***

****

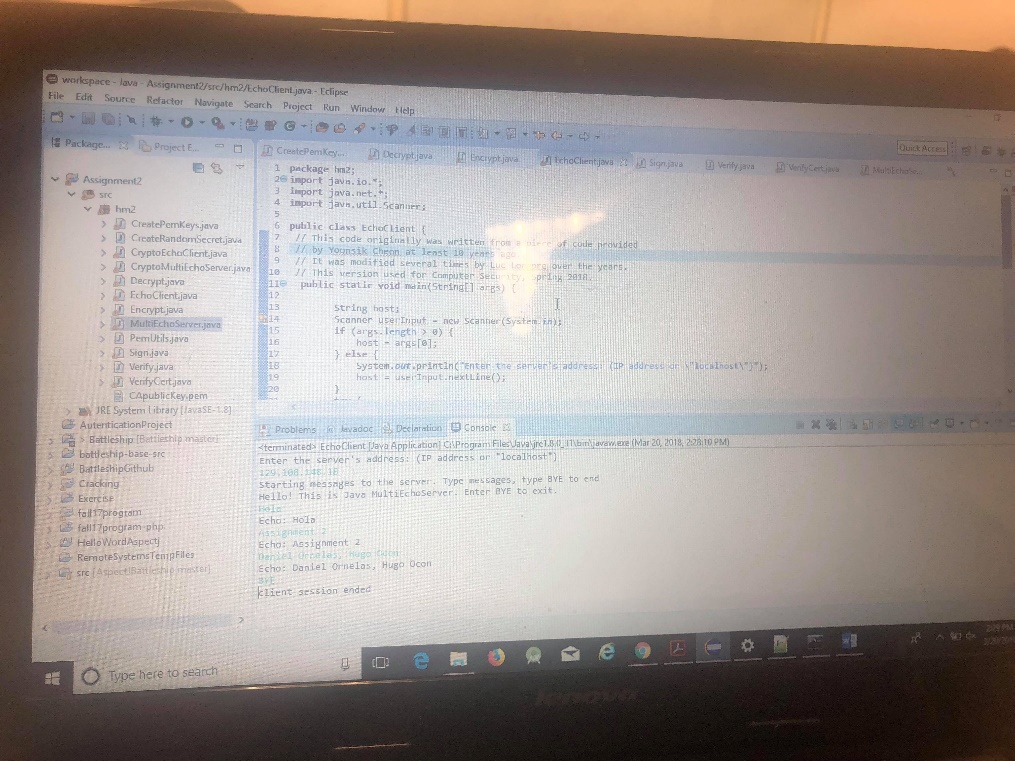
**Image 1 : VM Configuration**

****

**Image 2 : Same Machine Configuration**

****

**Image 3: Two-Machine Configuration A**

****

**Image 4: Two-Machine Configuration B**

For this part, I ran multiple tests. The first test was using a VM running Ubuntu. In a setup using NAT, the client could not connect to the server. In a configuration using bridged networks, the client running in the windows machine successfully communicated with the server running in ubuntu. For the same machine configuration, communication was successful between Eclipse running the client and IntelliJ IDEA running the server. For Two-Machine Configuration I contributed with Hugo Ocon. I ran the server in my machine, provided Hugo my IP address, and he ran the client in his machine. Communication was successful.

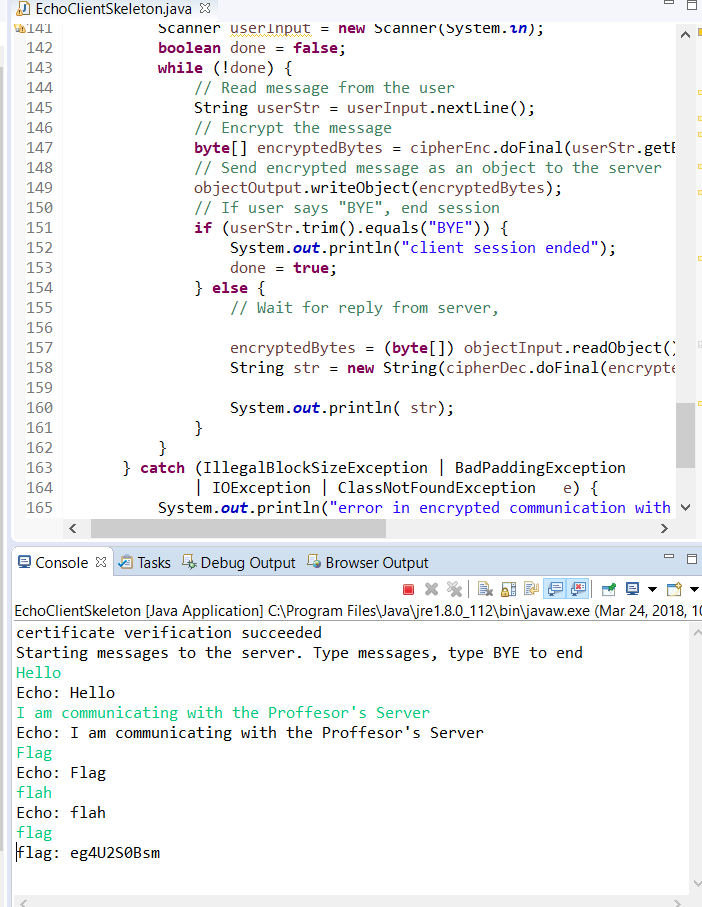
**Part 5**

The files MultiEchoServer and MultiEchoClient were modified to encrypt and decrypt communication in both ways. Files are provided in the zip file sent with this report.

**Part 6**

The program EchoClientSkeleton was modified to communicate with the Professor’s server using our protocol communication. The modified file is provided in the zip file.

The following is a screenshot of the program running :



**Part 7**

The flag received from the server was : eg4U2S0Bsm

**Feedback**

The assignment was great. I learned a lot from it as I had never used encryption with keys before. I think this assignment was very useful because we get an idea of how these methods work and if we want to follow a career in security, it is probable that we are going to use something similar. Parts 1-5 were easy, but it makes sense that they are easy because your are basically learning how everything works. Part 6 is challenging, but not hard if you really went step by step in the previous parts.

I worked in a group of 2 with Hugo Ocon. We did not contribute with any code or solution. Our only contribution to each other was to test the communication between two different machines.