Task :1

questions:

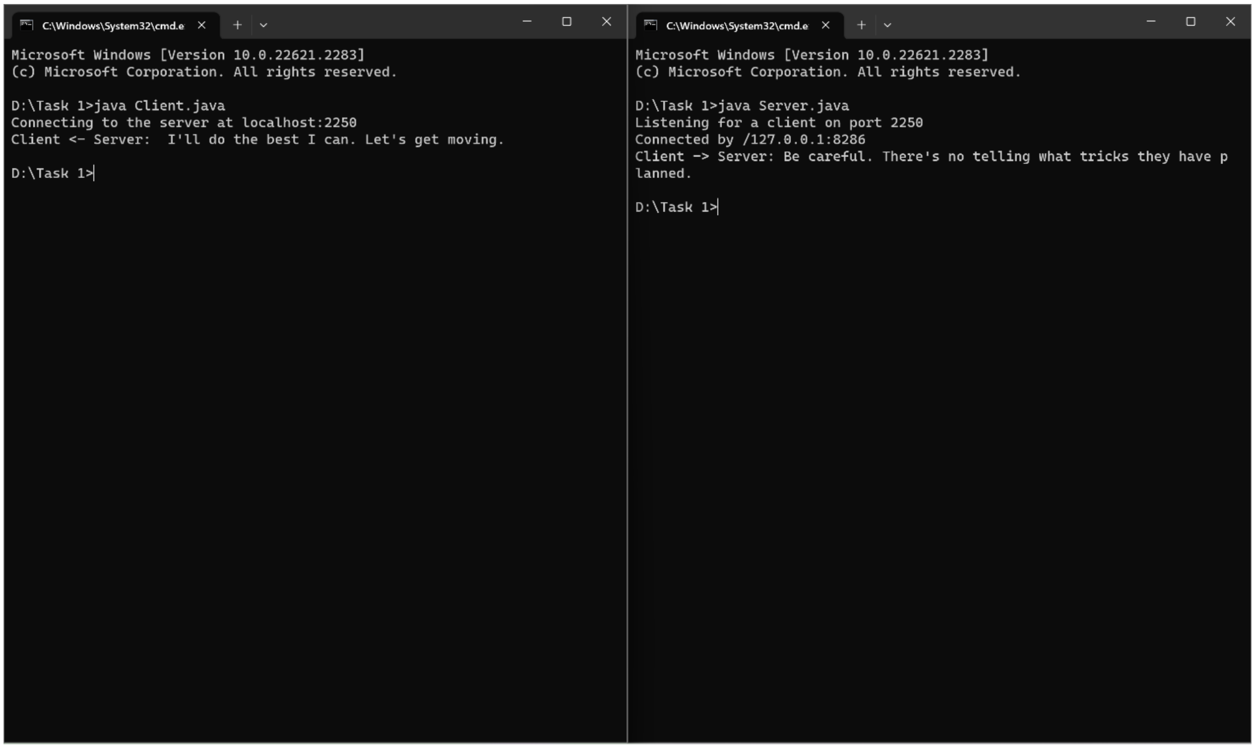
1. **What other potential security issues are there with this program? Identify and discuss at least three. (6 Marks)**
   Answer:
   Weak Cipher Suites: Cipher suites define the combination of cryptographic algorithms that are used in SSL communications. This includes the key exchange, bulk encryption, and the message authentication algorithms. When the program uses outdated or weak cipher suites
   It becomes susceptible to known cryptographic attacks.

   Certificate Expiry: Digital certificates, like those used in SSL, have a set validity period. This means they have a start date and an end date. The expiry date ensures that certificates are periodically checked and validated. Over a long time, a private key may get compromised, and by ensuring certificates expire, it limits the time an attacker can misuse a potentially compromised certificate.

   Vulnerabilities in the SSL implementation: The SSL protocol itself might be secure, but the actual software library implementing it can have bugs or vulnerabilities. If this happens
   It can expose the encrypted data to unauthorized individuals.

2. **If Barry were to secretly be the leaker, would the program remain secure? Explain why or why not.**
   Answer: The program would not remain secure. As Barry's CA certificate is used to sign and verify other certificates, now if Barry is compromised, he could generate fake certificates, which could facilitating man-in-the-middle attacks.

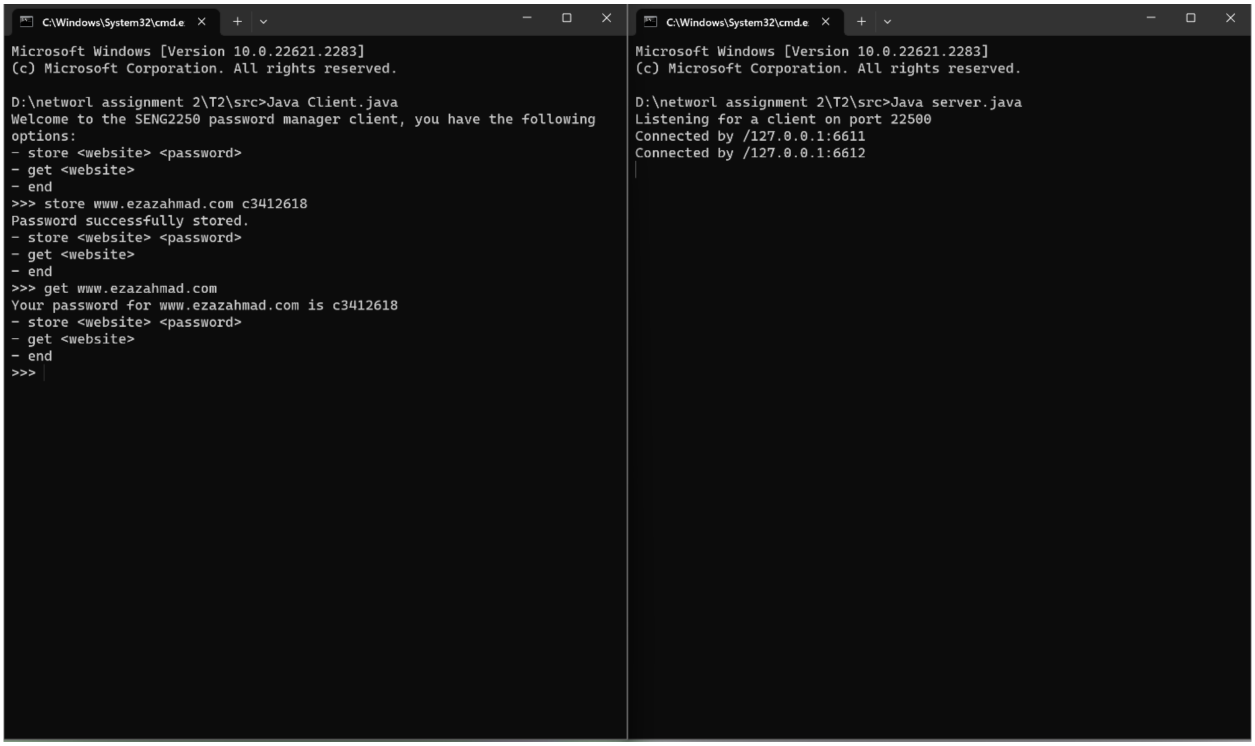
Program Execution Screenshot task-1:



```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

D:\Task 1>java Client.java
Connecting to the server at localhost:2250
Client <- Server:  I'll do the best I can. Let's get moving.

D:\Task 1>
```

```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

D:\Task 1>java Server.java
Listening for a client on port 2250
Connected by /127.0.0.1:8286
Client -> Server: Be careful. There's no telling what tricks they have p
lanned.

D:\Task 1>
```

<u>Program Execution Screenshot task-2:</u>



```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

D:\networl assignment 2\T2\src>Java Client.java
Welcome to the SENG2250 password manager client, you have the following
options:
- store <website> <password>
- get <website>
- end
>>> store www.ezazahmad.com c3412618
Password successfully stored.
- store <website> <password>
- get <website>
- end
>>> get www.ezazahmad.com
Your password for www.ezazahmad.com is c3412618
- store <website> <password>
- get <website>
- end
>>>
```

```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

D:\networl assignment 2\T2\src>Java server.java
Listening for a client on port 22500
Connected by /127.0.0.1:6611
Connected by /127.0.0.1:6612
```

<u>Task 1 reflection:</u>

On the task 1, I was immediately drawn into the critical realm of secure communications, an area of growing concern in today's digital age. The situation faced by Jill and Chris mirrored a real-world problem, emphasizing the vital need for robust encryption in any communication system.

To gain a comprehensive understanding of the task, I sought knowledge from various sources. Alongside our course materials, I delved into the labs and lecture slides, which served as a cornerstone for my foundational understanding. They provided theoretical insights and practical steps to address the challenges of SSL integration. Furthermore, I supplemented this knowledge with YouTube videos, which visually demonstrated the process of setting up and configuring SSL certificates. These videos helped bridge the gap between theoretical knowledge and its practical application, offering a more nuanced understanding of the subject.

Reflecting on broader implications, securing digital channels has vast real-world significance, from protecting corporate secrets to personal data. The methodology from this task could be seamlessly incorporated into myriad real-world scenarios, advocating for encrypted communications resistant to malicious intercepts.

In sum, Task 1 was more than an assignment, it was a window into the world of secure digital communications. By blending knowledge from lecture slides, labs, YouTube videos, and hands-on experimentation, I was better equipped to navigate the complexities of SSL and its real-world applications. This amalgamation of resources underscored the importance of a multifaceted learning approach, especially in the ever-evolving realm of cybersecurity.

Task 2 reflection:

Task 2 was a deep dive into the intricacies of password management and encryption, a task that made me appreciate the delicate equilibrium between user experience and foolproof security.

Starting off, the implementation of the RSA algorithm was indeed a daunting challenge. Though I had some basic understanding from our course materials, I found myself frequently referring back to labs and lecture slides, which were instrumental in reaffirming foundational concepts and providing guidance on proper implementation. To augment this, I explored a variety of online tutorials. These videos often presented different approaches to the RSA algorithm, enabling me to discern best practices and common pitfalls.

Building the user interface for the password manager was a vivid reminder of the importance of usability in cybersecurity. A potent security tool can become redundant if it's too complicated for end-users. Drawing from our lectures, it was evident that while creating a secure system is paramount, ensuring that it's intuitive and user-friendly is equally critical. Practical exercises from our labs, combined with insights from external videos, were especially beneficial in striking this balance.

Considering real-world implications, the essence of this task resonates strongly with the current digital landscape. With cyber-attacks becoming more sophisticated, the need for secure password management systems is pressing. The principles and methodologies employed in this task could serve as foundational elements for developing more advanced password managers.

In essence, Task 2 was a harmonious blend of theory and practice. While labs, lecture slides, and YouTube tutorials laid the groundwork, the actual implementation brought forth challenges that demanded innovative solutions. This project was not just an academic endeavor but also a glimpse into the complexities of real-world cybersecurity challenges.

Bibliography-

- Online videos
- Lectures slide
- Lab work