Configuration Manual

MSc Internship

MSc Cyber Security

Shirish Kumar Shrikant Jagdale
Student ID: x18146023

School of Computing
National College of Ireland

Supervisor: Mr Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Shirish Kumar Shrikant Jagdale

Student ID: X18146023

Programme: Msc Cyber Security **Year:** 2019-2020

Module: Academic Internship

Lecturer: Mr Imran Khan

Submission Due Date: 12th December 2019

Project Title: Secure sharing of secret key on insecure channel using Quantum Key Distribution

Word Count:925 **Page Count: 5**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Shirish Kumar Shrikant Jagdale
Student ID: x18146023

1 Introduction

This Configuration manual provides details about proposed model for securing the secret key. In this research a BB84 protocol of QKD is used for secure sharing of key. Along with secure sharing of key we have introduce another model in which MITM attack is performed. For running the code Java Eclipse platform is used, the process is divided into two section key sharing using QKD and Encryption /decryption process using AES. The key generated from key sharing process in QKD is later used for encryption and decryption process. Secure sharing of key using Quantum key distribution can be understood in following section.

2 System Configuration

This section provides over view of the system used for implementation of our proposed system

2.1 Hardware Configuration

Operating System: - Windows 10
Processor: 2 CPU
System: 64 bits
Hard drive: 1TB
Memory (RAM): 8GB

2.2 Software Configuration

For implementing our process code we have used following software.

Tool	Version	Description
JAVA	Java 8	It is software language basically use for designing various programs and applications
Eclipse IDE	2019-06	It is an Integral Development environment used in computer programming it consist of various plug-ins and customize environment [1]

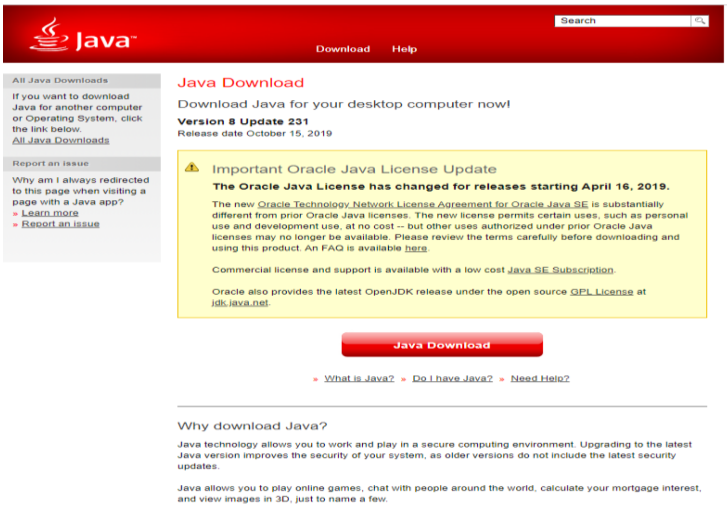
3 Working

In this section we will described about the working of our system what software needed and how to install them on system.

3.1 Software Installation

- Java software is downloaded using following link

  https://www.java.com/en/download/



All Java Downloads

If you want to download Java for another computer or Operating System, click the link below.
All Java Downloads

Report an issue

Why am I always redirected to this page when visiting a page with a Java app?
» Learn more
» Report an issue

Java Download

Download Java for your desktop computer now!

Version 8 Update 231
Release date October 15, 2019

Important Oracle Java License Update

The Oracle Java License has changed for releases starting April 16, 2019.

The new Oracle Technology Network License Agreement for Oracle Java SE is substantially different from prior Oracle Java licenses. The new license permits certain uses, such as personal use and development use, at no cost -- but other uses authorized under prior Oracle Java licenses may no longer be available. Please review the terms carefully before downloading and using this product. An FAQ is available here.

Commercial license and support is available with a low cost Java SE Subscription.

Oracle also provides the latest OpenJDK release under the open source GPL License at jdk.java.net.

Why download Java?

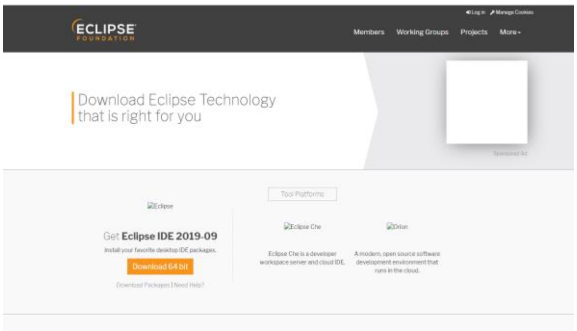
Java technology allows you to work and play in a secure computing environment. Upgrading to the latest Java version improves the security of your system, as older versions do not include the latest security updates.

Java allows you to play online games, chat with people around the world, calculate your mortgage interest, and view images in 3D, just to name a few.

Fig -1 Java website for downloading software

- Downloading Eclipse IDE for running the program.

  The Eclipse IDE can be downloaded from following website.
  https://www.eclipse.org/downloads/



Download Eclipse Technology that is right for you

Get **Eclipse IDE 2019-09**

Install your favorite desktop IDE packages.

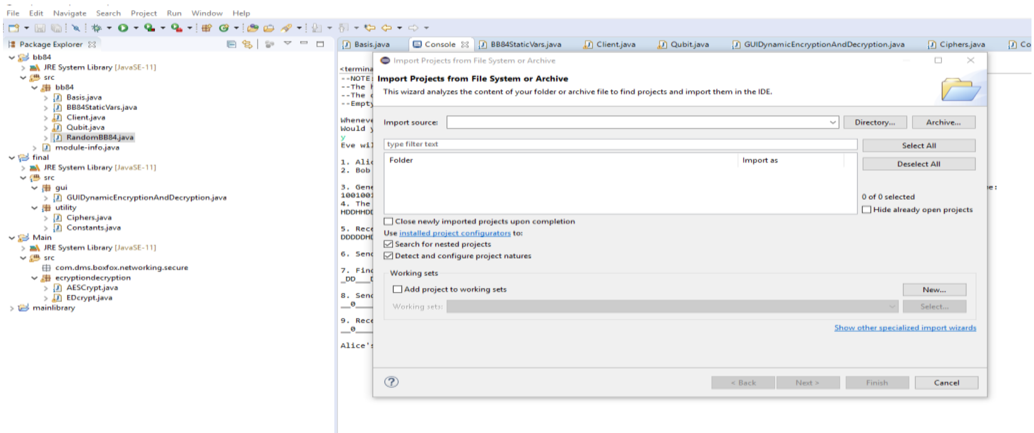
Eclipse Che is a developer workspace server and cloud IDE.

A modern, open source software development environment that runs in the cloud.

Fig-2 website for Eclipse IDE installation

3.2 Running the program for key sharing

To run the project first we have to open Eclipse IDE then to run the code. When eclipse is open, first go to menu bar click on file then import project from the file.



```
bb84
  JRE System Library [JavaSE-11]
  src
    bb84
      Basis.java
      BB84StaticVars.java
      Client.java
      Qubit.java
      RandomBB84.java
    module-info.java
final
  JRE System Library [JavaSE-11]
  src
    gui
      GUIDynamicEncryptionAndDecryption.java
    utility
      Ciphers.java
      Constants.java
Main
  JRE System Library [JavaSE-11]
  src
    com.dms.boxfox.networking.secure
    ecryptiondecryption
      AESCrypt.java
      EDcrypt.java
mainlibrary
```

Import Projects from File System or Archive

Import Projects from File System or Archive

This wizard analyzes the content of your folder or archive file to find projects and import them in the IDE.

Import source:

type filter text

Folder	Import as

0 of 0 selected

□ Hide already open projects

□ Close newly imported projects upon completion

Use installed project configurators to:

☑ Search for nested projects

☑ Detect and configure project natures

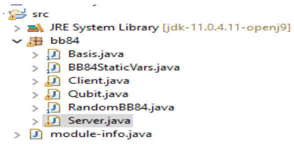
Working sets

□ Add project to working sets

Working sets:

Fig-3 Loading the project in IDE

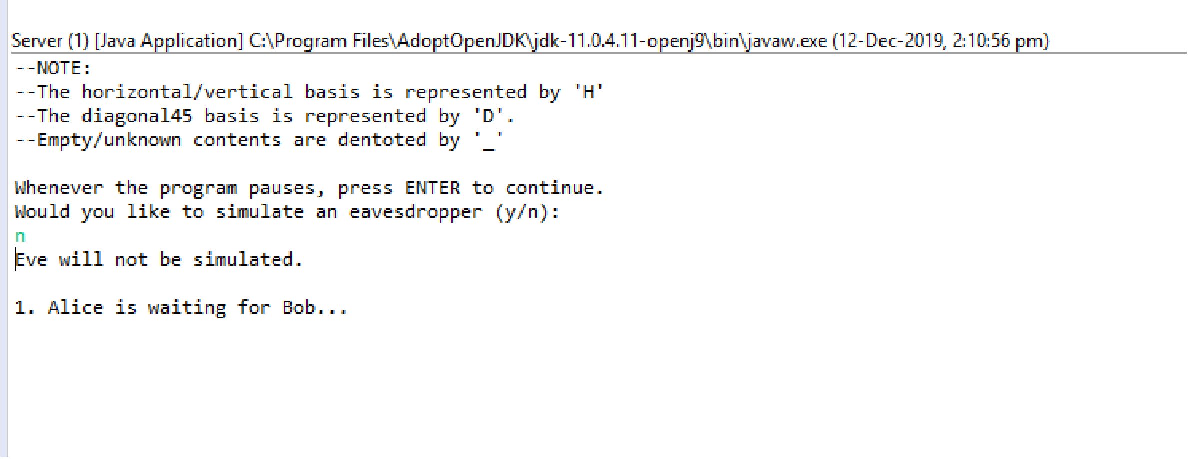
To import project click on directory go to path and load the project.Once the project is uploaded you will see all the java files present in package bb84.



```
src
  JRE System Library [jdk-11.0.4.11-openj9]
  bb84
    Basis.java
    BB84StaticVars.java
    Client.java
    Qubit.java
    RandomBB84.java
    Server.java
  module-info.java
```

Fig -4 side pannel of IDE

Once the project is uploaded first run the server file to get connection and you will get following message shown in figure.



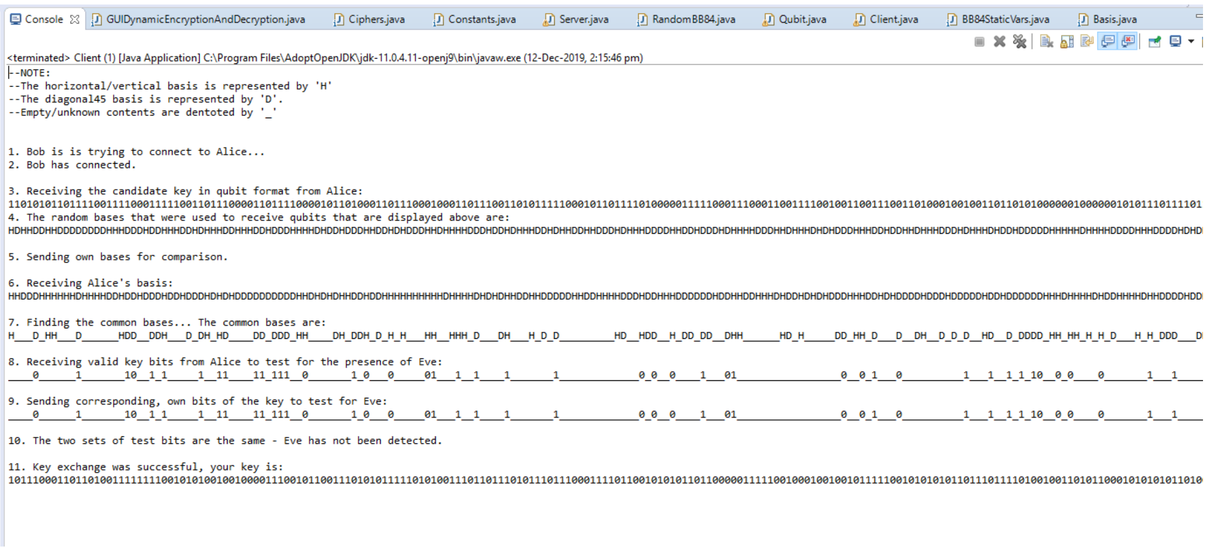
```
Server (1) [Java Application] C:\Program Files\AdoptOpenJDK\jdk-11.0.4.11-openj9\bin\javaw.exe (12-Dec-2019, 2:10:56 pm)
--NOTE:
--The horizontal/vertical basis is represented by 'H'
--The diagonal45 basis is represented by 'D'.
--Empty/unknown contents are dentoted by '_'

Whenever the program pauses, press ENTER to continue.
Would you like to simulate an eavesdropper (y/n):
n
Eve will not be simulated.

1. Alice is waiting for Bob...
```

Fig-5 Message received after server file is run

Select the choice of the process which you need to perform

If you type ‘n’ on console the program will run without introducing eve i.e. eavesdropper and program will wait for connection from Bob.

Then Run the client file to establish connection between server Alice and client Bob.



```
<terminated> Client (1) [Java Application] C:\Program Files\AdoptOpenJDK\jdk-11.0.4.11-openj9\bin\javaw.exe (12-Dec-2019, 2:15:46 pm)
--NOTE:
--The horizontal/vertical basis is represented by 'H'
--The diagonal45 basis is represented by 'D'.
--Empty/unknown contents are dentoted by '_'


1. Bob is is trying to connect to Alice...
2. Bob has connected.

3. Receiving the candidate key in qubit format from Alice:
110101011011110011110001111100110111000011011110000101101000110111000100011011100110101111100010110111101000000111110001110001100111100100110011100110100010010011011010100000001000000101011101111101
4. The random bases that were used to receive qubits that are displayed above are:
HDHHDDHHDDDDDDDDHHHDDDHDDHHHDDHDHHHDDHHHDDHDDDHHHHDHDDHDDDHHDDHDHDDDHHDHHHHDDDHDDHDHHHDDHDHHDDHHDDDHDHHHDDDDHHDDHDDDHDHHHHDDDHHDHHHDHDHDDDHHHDDHDDHHDHHHDHDDHDDHHDHHHDDDHDHHHDHDDHDDDDDHHHHHDHHHHDDDDHHHDDDDHDHD

5. Sending own bases for comparison.

6. Receiving Alice's basis:
HHDDDHHHHHHDHHHHDDHDDHDDDHDDHDDDHDHDHDDDDDDDDDDHHDHDHDHHDDHDDHHHHHHHHHHHDHHHHDHDHDHHDDHHDDDDHHDDHHHHDDDHDDHHHDDDDDDHDDHHDDHHHDHDDHDHDHDDDHHHDDHDHDDDDHDDDHDDDDDHDDHDDDDDDHHHDHHHHDHDDHHHHDHHDDDDHDD

7. Finding the common bases... The common bases are:
H___D_HH___D______HDD__DDH___D_DH_HD____DD_DDD_HH____DH_DDH_D_H_H___HH__HHH_D___DH___H_D_D_________HD__HDD__H_DD_DD__DHH______HD_H_____DD_HH_D___D__DH__D_D_D__HD__D_DDDD_HH_HH_H_H_D___H_H_DDD___D

8. Receiving valid key bits from Alice to test for the presence of Eve:
____0______1_______10__1_1_____1__11____11_111__0_______1_0___0_____01___1__1____1_______1_____________0_0__0____1___01_________________0__0_1___0__________1___1__1_1_10__0_0____0_______1___1____

9. Sending corresponding, own bits of the key to test for Eve:
____0______1_______10__1_1_____1__11____11_111__0_______1_0___0_____01___1__1____1_______1_____________0_0__0____1___01_________________0__0_1___0__________1___1__1_1_10__0_0____0_______1___1____

10. The two sets of test bits are the same - Eve has not been detected.

11. Key exchange was successful, your key is:
10111000110110100111111110010101001001000011100101100111010101111101010011101101110101110111000111101100101010110110000011111001000100100101111100101010101101110111101001001101011000101010101101010
```

Fig 6 output received when client file is run

And this is how you get your secret key. Then use the same key for encryption and decryption of text message.

3.3 Running the program for encryption and decryption

The key generated in previous section can now use for encryption and decryption of text message. For encryption and decryption the same process needs to be followed as done in previous section. The GUI dynamicEncryptionDecryption .java file should be run for execution of program.

Once the code debugged and run properly you will see a GUI on screen.

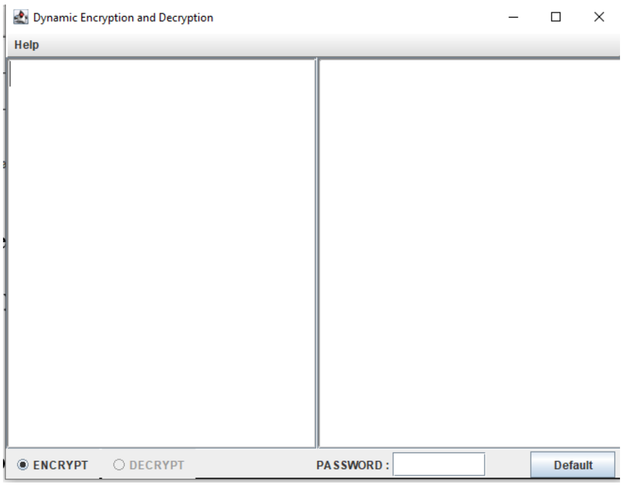
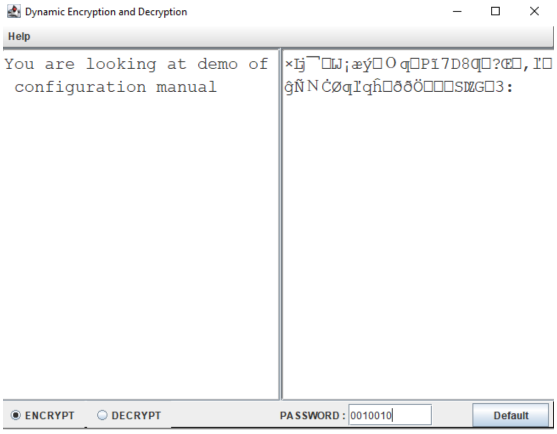


Fig -7 GUI for encryption and decryption process.

At the left size of the application we have to give plain text and at the right hand we will get corresponding cipher text when the key is put in password block.



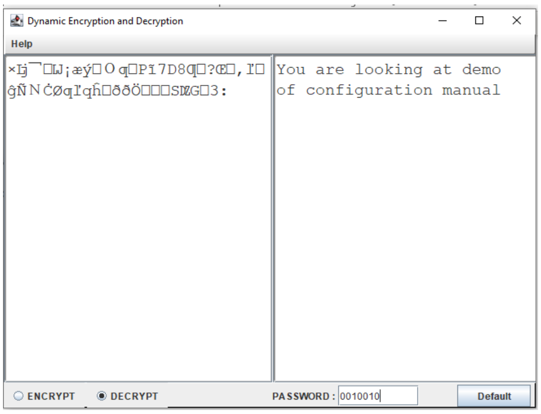
You are looking at demo of configuration manual

×ǈ¯□Ɯ¡æý□Oɋ□Pĩ7D8Ɋ□?Œ□,ľ□ĝÑNĊØɋľqĥ□ððÖ□□□SǱG□3:

● ENCRYPT ○ DECRYPT PASSWORD : 0010010

Fig -8 working of application (encryption)

For decryption of cipher text you choose the radio button ‘DECRYPT’ and hence at left most side you will see generated cipher text and when you put the same key you will get corresponding plain text.



×ǈ¯□Ɯ¡æý□Oɋ□Pĩ7D8Ɋ□?Œ□,ľ□ĝÑNĊØɋľqĥ□ððÖ□□□SǱG□3:

You are looking at demo of configuration manual

○ ENCRYPT ● DECRYPT PASSWORD : 0010010

Fig -9 working of application (decryption)

4 References

[1] "Eclipse," 10 12 2019. [Online]. Available: https://help.eclipse.org/kepler/index.jsp?topic=%2Forg.eclipse.platform.doc.isv%2Fguide%2Fint_eclipse.htm.