Bob 1

Mission 3 : QKD-encrypted Message

50 minutes of gameplay [60/200 points]

Your company is getting strong. Armed with this new technology, you now believe that this might work out to be the best, most 'in' way to communicate messages securely. A bit of backstory here, The founders of Alice and Bob are actually ambassadors of two warring countries. But secretly they are lovers. They want to send love letter to each other, and not to be misunderstood as spies. Now, it's time to fluorish their love... **The goal of this mission is to receive and decrypt QKD-encrypted messages from Alice.**

This mission is divided into smaller tasks, which consists of compulsory and optional tasks. The compulsory tasks are marked with either [Checkpoint], [Final Task], or [Secret Task] flags, while the unmarked tasks are sort of optional. It is thus a priority to complete all the flagged tasks before the optional tasks, as one will not be able to revisit these tasks after the deadline. The compulsory tasks are very important for the upcoming missions. It is also highly advisable to split the tasks among your teammates.

[10 points] [Checkpoint] Establish the secure key

> *We show here, however, that neither Bell's inequality nor EPR-correlated states are an essential part of the generation and certification of such a shared random secret.*
>
> *- BBM92*

Objective: Establish 32-bit secure keys by running an automated script.

Point allocation scheme:

- [Full] points upon completion of the objective

Step by step walkthrough:

1. Connect both classical device (from Mission 1) and quantum device (from Mission 2) to the same computer. Remember to enter the correct device addresses in `devloc_classical.txt` and `devloc_quantum.txt`.
2. Run the program `send_32bitQKD.py` (for Alice) and `recv_32bitQKD.py` (for Bob). Note that Bob needs to run his program first.
3. Patiently wait. The key should be ready in about 2 to 3 minutes, if everything works out smoothly.

[10 points] Message encryption handout

> *Privacy and encryption work, but it's too easy to make a mistake that exposes you.*
>
> *- Barton Gellman*

Objective: Complete the `Message Encryption` handout. No cheating or copying with Bob allowed [insert stern warning].

Point allocation scheme:

- Based on the number of correct responses in the handout.

Note: Only do this when there is a free time or there is a member in your group who happens to be free.

[10 points] Our setup handout

> *All experimentation is criticism. If an experiment does not hold out the possibility of causing one to revise one's views, it is hard to see why it should be done at all.*
>
> *- Sir Peter B. Medawar*

Objective: Complete the `Our Setup, Bandwidth` handout. No cheating or copying with Bob allowed [insert stern warning].

Point allocation scheme:

- Based on the number of correct responses in the handout.

Note: Only do this when there is a free time or there is a member in your group who happens to be free.

[20 points] [Final Task] Send encrypted message

> *Alone we can do so little; together we can do so much*
>
> *- Hellen Keller*

Objective: By using the secret key obtained earlier, correctly decrypt the encypted text sent by Alice. Note that you should not say the key or the message out loud, unless if being explicitly asked by `GameMaster`.

Point allocation scheme:

- [Full] points upon completion of the objective
- [20%] of total points reduction if any of the team member says either the keys or messages outload, and can be heard by the `GameMaster`

Step by step walkthrough:

1. Alice runs `encrpyt.py` to encrypt the message by using the established secure key.
2. Alice and Bob then both opens `chatting.py`, and Bob sets it on the listening mode. Alice then sends the encrypted text via the classical channel.
3. Bob then decrypt the received encrypted text by using `decrypt.py`.
4. If Bob thinks that he has obtained the correct message, he informs the `GameMaster`, and the `GameMaster` will check the correctness of the message with Alice.

Performed in the last 15 minutes of the session

[10 points] [Secret Task] Super secret messages, part 2

> *Good luck!*
>
> *- Ancient Wisdom*

There will be a few encrypted texts that you receive from Alice. You need to decrypt these texts and write the secret messages on the document given by the `GameMaster`. You have to **ensure the security of the content**, and that you **seal** the document and **return** it to the `GameMaster` after the conclusion of the mission. Listen to the explicit instructions from the `GameMaster` on when to receive each messages.

Objective: Bob successfully receives and decrypts all the messages from Alice.

Note: You must not communicate with Alice (no talking or signalling), except by using the softwares provided.

Point allocation scheme:

- [Full] points if all the messages is sent by Alice and received successfully by Bob, or
- A fraction of [full] points, proportional to the number of messages sent and received successfully.
- Some points will be forfeited if Bob communicates with Alice in any way besides through the softwares.