Bob 2 (Eve) - Mission 3: Cracking the secure messages

Qcamp 2019, Experimental Session 22/05/2019

50 minutes of gameplay [70/200 points]

Now, Charlie and Eve are officially a team. Both of you sign a memorandum of understanding (with Ethereum, of course) that you will work together and contrive to spy on Alice's messages. You heard from your informant that there will be a big "secret message" sending event soon. You want to obtain that message, and hopefully "blackmail" Alice and Bob. [Insert Evil laughter]. Good luck! **In this mission, you will work closely with Charlie to crack the secure messages that is sent by Alice to Bob.**

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] Listen

> ***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: Listen to every polarisation choices that Alice sends to Bob.

Point allocation scheme:

- [Full] points after completion of the mission.

Step by step walkthrough:

1. Hack the quantum channel through the same procedure described in `Mission 2`. You should have intercepted an integer multiple of 16-bits. Obtain the polarisation state sequence.

[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 Charlie allowed.

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 from Charlie 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] Listen and collaborate

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

Objective: Collaborate with Charlie to decrypt the message that is sent by Alice to Bob. You will need to successfully decrypt the message at least once.

Point allocation scheme:

- [Full] points after completion of the mission.

Step by step walkthrough:

1. For each bit, Alice and Bob would have agreed as to whether they would actually use that bit. This results in a string of `0` and `1` that encode the agreement. Charlie will intercepted this so-called `mask`. Use this `mask` to sift the polarisation state sequence for the secret key.

Performed in the last 15 minutes of the session

[20 points] [Secret Task] Super secret messages, encrypted

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

Alice is sending some super sensitive messages to Bob. Hack it! The `GameMaster` will tell you when the secret messages are being sent. After receiving all the message, **write it down** in the **super secret document** and pass it to the `GameMaster` after the conclusion of the mission.

Objective: Your team successfully decrypts all the secret messages that Alice sends to Bob.
Point allocation scheme:

- [Full] points if you successfully decrypt all the messages.
- A fraction of [full] points, proportional to the number of correctly decrypted messages.