

## Mission 2 : Setting Up Quantum Key Distribution

---

*70 minutes of gameplay [60/200 points]*

As you progress through this company start-up, you start to suspect from quantum physicists that classical communication is probably not very secure. Well, you have gone through a full week of Quantum Wierdness and whatnot lectures.

You want to develop a scheme from the lectures: The BB84 QKD scheme. However, as you are just a start-up company, you do not have a lot of money, so you can not buy single photon detectors. Also, your friend, who is an expert in popular science, convince you that you don't need single photons. Well, as you don't have much choice anyway, you will just try it loh.

**The goal of this mission is to establish the quantum link between Alice and 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.

### [20 points] [Checkpoint] Align the polarisation

*Why would you want to use less to send information. Wouldn't more photons guarantee a stronger signal?*

*- Your good friend, Dr. Emmet Brown*

Objectives:

1. Align the polarisation between Alice and Bob, and
2. Obtain the intensity matrix, with signal degradation less than 0.2.

Point allocation scheme:

- [Full] points upon completion of the objectives
- [80%] of total points upon completion of the objectives, but with the signal degradation higher than 0.2.

Step by step walkthrough:

1. Run the polarisation alignment GUI program, and blah blah..
2. Run the intensity matrix program

## [20 points] [Checkpoint] Without the electronics, there is NONE

*Resistor: I'm gonna ask you this one time, where is the circuit?*

*Transistor: Yeah, I'll do you one better, WHO is the circuit?*

*Diode: I'll do YOU one better, WHY is the circuit?*

*- 1 divided by 0*

Objective: Construct a circuit capable of sending IR signals to Bob (while at the same time Bob needs to construct another circuit capable of receiving the IR signals). The objective is accomplished when Alice successfully sends (and Bob successfully receives) the blinking signal.

**Very important notes:** Read the safety precautions in Section 1.2.1 of the technical documents. This is *extremely important*, as you will get tested about this at the end of the session (no joking, confirm plus chop!).

Point allocation scheme:

- [Full] points upon correct, efficient, and stable implementation of the circuit, or
- [80%] of total points upon successful implementation of the circuit, but not necessarily correct, efficient, nor stable.

Step by step walkthrough:

1. Gather all the necessary components, and note down the polarity and the pin assignments. The facilitator will give a short lecture and demonstration about breadboard, but in case you miss it, you can refer to Section 1.2.3.
2. Construct the circuit according to BREAK the ice, STOMP the ground, LIFT the airthe diagram, noting the polarity and the pin assignment. *If the polarity or pin assignment is incorrect, you might burn the components.* If you are unsure about certain stuffs, ask the facilitator.
3. Upload the Arduino program `ArduinoClassical.ino` to the correct device. You might want to use terminal command `dmesg` to look for the device address, typically in the form of `/dev/ttyACM0` or `/dev/ttyUSB0`.
4. After finish uploading, you can open the serial monitor with `Shift+Ctrl+M`. Try to send `HELP` to the Arduino, and look at the reply. Try to send blinking signal with `SBLINK` (for Alice), or receive blinking signal with `RBLINK` (for Bob). For Alice, you should be able to see the blinking IR light with your phone camera (except iPhone). For Bob, you should see the indicator light blinking, and the serial monitor prints `BLINK!`. You may also ask the `GameMaster` to help sending/receiving IR signals from the main computer.
5. Try to perform the similar experiment, but now with Alice/Bob instead. Remember to position the sender and receiver roughly in the line of sight.

## [10 points] Computer does not speak words

*The answer to the ultimate question of life, the universe and everything is 42.*

*Technically, it is 0b101010.*

This pedagogical exercise will dwell a little bit deeper into how information is actually sent. Most implementations deal with binaries, which is a string of 1 and 0's. Then, how can we write numbers, words, symbols, or even emojis in this binary string?

Objective: Alice writes the message "Hello Qcamp!" in binary representation, and sent it to Bob. You will need to use the programs in **BinaryComm Package** to perform this task, and you will also need to complete the **conversion table form**. To get full points, both Alice and Bob must participate in this exercise.

Point allocation scheme:

- [Full] points when both Alice and Bob successfully completed the task, or
- [50%] of total points, if Alice takes part and completes her conversion table form.

Step by step walkthrough (optional):

1. Upload the Arduino program `send_binary.ino` (for Alice) and `recv_binary.ino` (for Bob).
2. For Alice, convert each character from ASCII to binary, and complete the conversion table form. You can use the ASCII table, but the program `conv_ascii.py` might also be useful.
3. For Alice, send each character (in binary form, i.e. `01010101`) through the serial monitor. Note that you can only send one character (one byte, 8 bits) at a time. For Bob, prepare to listen to what Alice sends via the serial monitor.
4. For Bob, after successfully receiving all the characters, convert them from binary to ASCII and complete the conversion table form.

## [10 points] Asymmetrical cryptography handout

*When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.*

*- John Perry Barlow*

Objective: Complete the "asymmetrical cryptography 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] Let's chat with Bob

*The Internet: transforming society and shaping the future through chat.*

- Dave Barry

Objectives:

1. Successfully communicate a message to Bob via the IR link by using the program `send_message.py` ,
2. Help Bob to construct the IR sender circuit, and
3. Chat with Bob (i.e. send a few messages back and forth) by using the program `chatting.py` .

Point allocation scheme:

- [Full] points by completing all the objectives **within 75 minutes** from the start of Mission 1 (leaving 15 more minutes to wrap up other tasks), or if fails,
- [80%] of total points by completing all the objectives within the time limit, or if fails,
- Maximum of [80%] of total points, proportional to the effort and the number of completed tasks at the end of the time limit.

Step by step walkthrough:

1. First, test the fidelity of the signal. Alice can run `send_testQ.py` and Bob can run `recv_testQ.py` . The programs will just send and receive `Qc!8` repeatedly. Note that you might need to modify the device address at `devloc.txt` .
2. To try sending a longer messages, Alice can run `send_message.py` and Bob can run `recv_message.py` .
3. To construct a two way communication, Alice needs to build a receiver circuit and Bob needs to build a sender circuit. Alice's member (who is now a professional) can help Bob's member in building the sender circuit, and vice versa.
4. After building them, repeat the above procedures: send and receiving blinking signal, test for signal fidelity, and test to send a message (but now in the other direction).
5. If everything works nicely, both Alice and Bob can run `chatting.py` . Bob can turns into listening mode by pressing an `Enter` button. The chatting should happens both ways.

## ***Performed after the conclusion of Mission 1:***

### **[10 points] [Secret Task] A super secret message**

*After Mission 1, a secretive agent approaches your company, and she is interested in sending some super secret messages to her accomplice which lives close to Bob. She is very certain that the IR channel is quite secure, but is it?*

There will be a few messages that you need to send to Bob within 10 minutes after the conclusion of Mission 1. They will come in a secret document from 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 send each messages.

Objective: Alice successfully sends all the messages to Bob.

Note: You must not communicate with Bob (no talking or signalling), except by using the chatting software developed in Mission 1.

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 Alice communicate with Bob in any way besides the chatting software.