# Exercise 1
# Attack Modeling

COMP 5900 - Winter 2016

January 5, 2016

Adapt the MATLAB class `channel` of the QKD example to simulate the following attack. The adversary (i.e., Eve) implements the *intercept and resend* attack. The adversary has no access to the polarization bases chosen by the encoder (i.e., Alice). For each photon, the adversary randomly selects a measurement basis, measures and resends a new photon according to the measurement.

Simulate the protocol for random sequences of bits of lengths 10 to 100, in steps of 10 bits. Simulate each case at least 1,000 times. As a function of the length of the random sequence of bits, calculate and plot the following rates:

1. Key establishment success.
2. Interception success
3. Both key establishment success and interception success at the same time.

In few words, write your conclusions.
**Due date:** January 18, submit you work on cuLearn (your program, sample execution, with random data, and plots).