# Introduction to Quantum Mechanics
# Homework Eight

College of the Atlantic

**Due Friday 6 June, 2014**

1. Encrypt the following plaintext message `THE BEARS ARE VERY SAD.` For the key, use the description for course HS784, *Communicating Science*.

2. Decrypt the following message: `LCJROSZGGKGQFTME`. The key is the description for course HS728 *Economic Development: Theory and Case Studies*.

3. Alice and Bob are using an EPR experiment to distribute a key for a cipher using the protocol we discussed in class and described in chapter 13 of Styer's book. Alice observes:

$$\texttt{A1 B1 B0 A0 C0 \quad A0 C1 B0 B1 C1 \quad A1 A0 C1 C0 B0 \quad A0 C1 A0 C0 C1} \tag{1}$$

   While Bob observes:

$$\texttt{B0 B0 C0 C1 A1 \quad B1 C0 B1 B0 A0 \quad C1 B1 C0 B0 C0 \quad A1 B0 A1 C1 C0} \tag{2}$$

   What key would Alice and Bob end up using? Was Eve listening in? How can you tell?

4. (Use wolframalpha to help you with these computations.) Suppose Alice and Bob are using an RSA public-key encryption to send a message from Bob to Alice. Suppose Alice chooses $p_1 = 97$ and $p_2 = 89$. They agree to use $e = 5$ as the exponent.

   (a) What number $n$ will Bob and Alice use as the modulus for their calculations?

   (b) What number $d$ would Alice use to decrypt Bob's message? When figuring out $k$, you will need to set $k = 3$ to ensure that $d$ is an integer.

   (c) Suppose Bob wants to send the message $m = 71$ How would he encrypt it? That is, what is $c$?

   (d) Show that if Alice decrypts Bob's encoded message, she will get 71. That is, show that $c^d = 71$.

   (e) Why would it be very hard for Eve to figure out $d$?