

Physics III
Homework Nine
Due Friday 1 June, 2007

1. Krane, Chapter 4, Problem 4.
2. A message was sent using the one-time pad shown below. The coded message is QCZDICIJTBEHXNZZ. What is the decoded message? Show at least some of your work to make it clear how you're decoding the message.

9	2	4	25	8	22
17	5	19	18	12	3
22	1	21	8	11	20
2	2	19	6	20	9
0	5	21	7	13	10

3. Alice and Bob are using an EPR experiment to distribute a key for a Vernam cipher using the protocol we discussed in class. Alice observes:

$$A1 B1 B0 A0 C0 \quad B0 A1 B0 B1 C1 \quad A1 A0 C1 C0 B0 \quad C1 B1 A0 A0 A1 \quad (1)$$

While Bob observes:

$$B0 B0 C0 C1 A1 \quad B1 C0 B1 B0 A0 \quad C1 B1 C0 B0 C0 \quad A1 B0 A1 C0 C0 \quad (2)$$

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