This exam is intended to take no more than 70 minutes. I am allowing 150 minutes to account for typing/recopying of solutions, technical problems, etc.

The exam is open-book and open-note — meaning:

- You may use all of this course's resources: the Mermin textbook, your class notes, your old homework, and the course web/Moodle site. You may not share any resources with any other person while you are taking the exam.
- You may cite material (definitions, theorems, examples, algorithms, etc.) from class, the assigned textbooks readings, and the assigned homework problems. You do not have to redevelop or reprove that material. On the other hand, you may not cite results that we have not studied.
- You may not consult any other books, papers, Internet sites, etc. You may use a computer for viewing the course web/Moodle site, typing and running Python programs of your own creation, typing up your answers, and e-mailing with me. If you want to use a computer for other purposes, then check with me first.
- You may not discuss the exam in any way — spoken, written, etc. — with anyone but me, until everyone has handed in the exam.

I will try to check my e-mail frequently during the exam period. Feel free to ask clarifying questions. If you cannot obtain clarification on a problem, then explain your interpretation of the problem in your solution. Never interpret a problem in a way that renders it trivial. Check your e-mail occasionally, in case I send out a correction.

Your solutions should be thorough, self-explanatory, neat, concise, and polished. Always show enough work and justification so that a typical classmate could understand your solutions. Correct answers without supporting work rarely earn full credit. You might want to work first on scratch paper and then recopy your solutions. Alternatively, you might want to type your solutions. If you cannot solve a problem, then write a brief summary of the approaches you've tried. Partial credit is often awarded. Present your solutions in the order assigned.

Good luck. :)

A. Consider the following modification to the Bennett (1992) key exchange protocol. Instead of everyone (Ariko, Babatope, and Einar) knowing that Ariko encodes $|0\rangle$ and $|1\rangle$ into $|0\rangle$ and $|+\rangle$ respectively, everyone knows that she encodes $|0\rangle$ and $|1\rangle$ into $|0\rangle$ and $|\omega\rangle$, respectively. Here, $|\omega\rangle$ is an arbitrary one-qbit state, agreed upon in advance and known to everyone.

A.A. How does this change affect Babatope's end of the protocol? What must he do differently than in the usual $|\omega\rangle = |+\rangle$ case?

A.B. What makes any particular choice of $|\omega\rangle$ good or bad (and for whom)?

B. Suppose that I have a two-qbit state $|\psi\rangle$ and I perform partial measurement of the second qbit. What is the probability that I observe $|1\rangle$ on the second qbit?

C. Suppose that we feed $|10\rangle$ into Deutsch's algorithm instead of the usual $|11\rangle$ (without modifying any other part of the algorithm). Does this modified algorithm still solve Deutsch's problem, or does it solve some other problem, or is it of no value?

D. Using algebraic properties of the tensor product, prove that, if U and V are unitary matrices, then $U \otimes V$ is also unitary.