MTH6115 Cryptography Exercises 5

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Friday 13/3/09.
Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.*

Q1 Consider the following decision problem.

INVERTIBLE: Given an $n \times n$ matrix A each of whose entries is either 0 or 1, is A invertible?

(a) Describe an instance of INVERTIBLE and determine its size.

(b) Describe a certificate for verifying a 'yes' answer to INVERTIBLE which can be checked in polynomial time.

(c) Describe a certificate for verifying a 'no' answer to INVERTIBLE which can be checked in polynomial time.

(d) Does INVERTIBLE belong to the complexity class P? Give a brief justification for your answer. [40]

Q2 (a) Find the orders of 2 and 3 in $\mathbb{Z}_{41}$. [20]

(b) Use (a) to construct a primitive root modulo 41. [10]

Q3 Consider the following decision problem.

PRIMITIVE: Given a prime p and an integer x, $1 \leq x \leq p-1$, is x a primitive root modulo p?

(a) Show that we can solve this problem by calculating $x^t \bmod p$ for all $1 \leq t \leq (p-1)/2$. [10]

(b) Is the algorithm in (a) a polynomial time algorithm for solving PRIMITIVE? Why? [10]

Q4 Let n be a positive integer. Prove that $\lambda(n)$ divides $\phi(n)$. [10]