EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework #06 **Professor Dunham**
27 Feb 2020 **Due: 5 Mar 2020**

Suggested Reading in Menezes, Oorschot and Vanstone: Chapter 2.
http://en.wikipedia.org/wiki/Turing_machine

1. The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^{c*n^{1/3}(\log_2 n)^{2/3}}$. Assuming 4GHz computers and $c = 1$ (and the units of the given expression are clock cycles), estimate the size of the numbers that cannot be factored for the next 100 years.

2. Verify that the knapsack problem is equivalent to the 0-1 integer programming problem by showing that every knapsack problem can be cast into a 0-1 integer programming problem and *vice versa*.

3. You are given the following knapsack problem. Find a solution to the problem (there is at least one).

$$\begin{array}{ll} a_1 = 543{,}719 & a_2 = 47{,}812 \\ a_3 = 319{,}982 & a_4 = 921{,}645 \\ a_5 = 13{,}247 & a_6 = 87{,}658 \\ a_7 = 376{,}926 & a_8 = 193{,}275 \\ a_9 = 439{,}261 & a_{10} = 775{,}327 \end{array}$$

$$b = 1{,}377{,}256.$$

4. Assuming the conventions used in Handout #06 on Deterministic Turing Machines (DTMs), write a program for a DTM which when given the integer n computes $3n + 2$.

5. You are given the algorithm for two Deterministic Turing machines. Determine what function each algorithm implements, assuming the conventions used in Handout #06 on Deterministic Turing Machines. Also, determine an upper bound on the complexity of the algorithm using $O(f(n, m))$ notation where n and m are integer inputs to the algorithm.

(a). The tape input is a pair of integer numbers

Scan R to 1st 0 and write 1.
Scan R to 1st 0 and write 1.
Scan R to 1st 0 and write 1.
Scan R to 1st 0 and write 1.
Scan L to 1st 0 and write 1.
Halt.

(b). The tape input is a single integer number.

Scan R to 1st 0.
Write 1.
Move R one.
Write 1.
Move R one.
Write 1.
Move R one.
Write 1.
Scan L to 1st 0.
Move R one.
Halt.