GEORGIA INSTITUTE OF TECHNOLOGY
School of Electrical and Computer Engineering

ECE 6280
Cryptography

HWK #1, Due: Thursday Jan. 23

Problem 1: Solve the question 1.27 from Chapter 1 of the textbook.

Problem 2: Find an upper bound for the number of bit operations required to compute $n!$.

Problem 3: Using the big-O notation, estimate the number of bit operations required to multiply an $r \times n$ matrix by an $n \times s$ matrix, where all matrix entries are less than or equal to m.

Problem 4: Let $\mathcal{P}_1$ be the problem:

Input: A polynomial $p(x)$ with integer coefficients.

Question: Is there any interval of the real number line on which $p(x)$ decreases?

Let $\mathcal{P}_2$ be the problem:

Input: A polynomial $p(x)$ with integer coefficients.

Question: Is there any interval of the real number line on which $p(x)$ is negative?

Show that $\mathcal{P}_1$ reduces to $\mathcal{P}_2$.

Problem 5: An affine block cryptosystem is one in which the key is a nonsingular square $d \times d$ matrix A together with a d-vector t. It works by breaking the message up into binary blocks of size d, then:

$$C = AM + t$$

where M is a particular block of length d and all arithmetic is modulo 2.

(a) Show that the number of keys is $2^d(2^d - 1)(2^d - 2) \cdots (2^d - 2^{d-1})$.

(b) Prove that the cryptosystem is vulnerable to chosen plaintext attack, and find the minimum length of plaintext-ciphertext needed to find the key.

Problem 6 (optional): Let b, N and m be integers such that $b < m$. Show that the number of bit operations required to compute $b^N \mod m$ is $O(k^2\ell)$ where k and ℓ are the lengths of m and N respectively. [Hint: write $N = c_{\ell-1}2^{\ell-1} + c_{\ell-2}2^{\ell-2} + \cdots + c_1 2 + c_0$ and use repeated squaring techniques (calculate $b^{c_j 2^j} \mod m$ from $b^{c_{j-1}2^{j-1}} \mod m$)].