GEORGIA INSTITUTE OF TECHNOLOGY
School of Electrical and Computer Engineering

ECE 6280
Cryptography

HWK #4 and 5, Due: Thursday April 3, 2014

Problem 1-7 Solve questions 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.23 from the textbook (Third Edition).

Problem 8: Suppose you, as a cryptanalysis were interested in an RSA modulus n, and you are given a t such that $a^t \equiv 1 \mod n$ for all $a \in \mathbb{Z}_n^*$. (Note that t is not necessarily $\phi(n)$. In the case $n = 69841$, $\phi(69841) = 69630$, but t could have many other values including 2310 and 138600.)

(a) Give an efficient randomized algorithm for factoring n.

(b) What is the probability of success for the algorithm you found in part (a). Explain why?

Problem 9: Implement the Pohlig-Hellman algorithm for finding discrete log problem in $\mathbb{Z}_p$, where p is prime and α is a primitive element. Use your program to find $\log_5 8563$ in $\mathbb{Z}_{28703}$. Submit the print of your code.