

CSCI 303 Homework 6

Problem 1 (31.1-1):

Prove that there are infinitely many primes.

Problem 2 (31.1-7):

For any integer $k > 0$, we say that an integer n is a *kth power* if there exists an integer a such that $a^k = n$. We say that $n > 1$ is a *nontrivial power* if it is a *kth power* for some integer $k > 1$. Show how to determine if a given β -bit integer n is a nontrivial power in time polynomial in β .

Problem 3 (Derived from 31.2-2):

Use the extended-Euclid's algorithm to compute $\gcd(899, 493)$ and numbers x and y such that $899x + 493y = \gcd(899, 493)$. Show your work.

Problem 4 (Not in book):

Your RSA private key is $\langle 7, 33 \rangle$. Digitally sign the message $M = 9$. Show your work.

Problem 5 (31.7-1):

Consider an RSA key set with $p = 11$, $q = 29$, $n = 319$, and $e = 3$. What value of d should be used in the secret key? What is the encryption of the message $M = 100$? Show your work.