06-88-447: Computer Networks and Security, Summer 2017

Assignment three (Due: Wednesday July 5, 2017)

1.-4. Problems from the textbook (7th Edition): 9.2(d), 9.2(e), 9.4, and 9.7.

5. Bob setup an RSA system by choosing $p = 13, q = 17$, and $n = 187$. Bob selects the public key as $e = 11$. Alice would like to send Bob a secret message $m = 2$. Compute $c = m^e \bmod n$ using the three modular exponentiation methods given in lecture notes on Chapter 5 at Pages 12, 13, and 21. List the intermediate results of x and y for each loop value of i.

6. Problems from the textbook (7th Edition): 11.6

7. Consider the following hash function that takes an input x of arbitrary size and produces a 160-bit output $h(x)$: Let x be a binary number. Then $h(x) = 2^{159} + (-x) \bmod 2^{159}$. Check whether or not $h(x)$ satisfies the properties for a good cryptographic hash function listed at Page 6, Lecture notes on Chapter 6.

8. Problems from the textbook (7th Edition): 12.2