

CMPS 111 Fall 08 Homework 4

Assigned: Tues, Nov 25

Due: Tues, Dec 2, 11:59pm

1. Problem 4.10, from the book.
2. Problem 4.14, from the book.
3. Problem 4.16, from the book.
4. Problem 4.20, from the book.
5. Problem 4.24, from the book.
6. Problem 4.26, from the book.
7. Problem 4.28, from the book.
8. Problem 4.32, from the book.
9. Problem 4.33, from the book.
10. Problem 4.36, from the book. *Hint:* use *find*, dump to a file, run a post-processor.
11. An RSA (Rivest-Shamir-Adelman) cryptosystem is composed of $e, d, n = pq$ and where $d \times e \equiv 1 \pmod{\varphi(n)}$. Construct a simple RSA cipher using these parameters: $p = 3, q = 5, e = 11$, and $d = 3$. The public key is e , the private key is d , n is also public but p, q and $\varphi(n)$ are private.
 - (a) $n = \underline{\hspace{2cm}}$ and $\varphi(n) = \underline{\hspace{2cm}}$.
 - (b) If the adversary knows $\varphi(n)$ then it is trivial to compute ____.
 - (c) The formula for $\mathcal{E}(m) = \underline{\hspace{2cm}}$ and for $\mathcal{D}(c) = \underline{\hspace{2cm}}$.
 - (d) Why is it safe for n to be made public?
12. A Diffie-Helman key exchange requires a base a , and a prime p . A must choose an x and B must choose a y . It then proceeds as follows:

$$A \rightarrow B : a, p, a^x \pmod{p}$$

$$B \rightarrow A : a^y \pmod{p}$$

- (a) What secret do A and B now share?
- (b) Why doesn't the adversary also know this secret?
- (c) What would be necessary for the adversary to learn this secret?