Shashank Karthikeyan
A50703012

CSE 201 Homework #6

1. The focus of chapter 4 is cryptography. The main method that the book talks about in this chapter is the shared secret method. The book uses a simple analogy to explain it. Let there be 3 people in a room. You, Arnold and Eve. You want to send an encrypted message to Arnold without Eve find out what it is. So firstly, you and Arnold have agreed on a shared secret number before entering the room. Then you take the number you want to tell him, add that to the secret number and tell it to him. He will then subtract the secret number to get the message. Even if Eve hears the encrypted message she doesn't know the secret number so she can't decrypt it. The book then talks about establishing a shared secret in public. One simple way they showed is that each of you choose a private number. Then you agree upon a shared public number and multiply your public number by your private number to get your public-private number (PPN). Then you share your PPN with each other and multiply your private number with the other's PPN. After this process, both of you will have the same number. This is a simple version of what occurs. In the real world, there is much more complex arithmetic involved since simpler methods can be "hacked" using brute force. The more complex methods will require an insane amount of time to be cracked using pure brute force.

2. Remainder in parenthesis
    a. 8888/2 = 4444(0)/2 = 2222(0)/2 = 1111(0)/2 = 555(1)/2 = 277(1)/2 = 138(1)/2 = 69(0)/2 = 34(1)/2 = 17(0)/2 = 8(1)/2 = 4(0)/2 = 2(0)/2 = 1(0)/2 = 0(1) → $\mathbf{10001010111000_2}$
    b. 2555/6 = 425(5)/6 = 70(5)/6 = 11(4)/6 = 1(5)/6 = 0(1) → $\mathbf{15455_6}$
    c. 8990/19 = 473(3)/19 = 24(Q)/19 = 1(5)/19 = 0(1) → $\mathbf{15H3_{19}}$
3. $4645_9 = 4(9^3)+6(9^2)+4(9)+5 = \mathbf{3443_{10}}$
4. Carry's in parenthesis
    a. 5665+4664 = $\mathbf{13662_7}$
        i. 5 + 4 = 2(1)
        ii. 6+6+1 = 6(1)
        iii. 6+6+1 = 6(1)
        iv. 5+4+1 = 3(1)
        v. 0+1 = 1
    b. AB56+9868 = $\mathbf{143BE_{16}}$
        i. 6+8 = 14 = E
        ii. 5+6 = 11 = B
        iii. B+8 = 11+8 = 3(1)
        iv. A+9+1 = 10+9+1 = 4(1)
        v. 0+1 = 1
5. $201.201_3 = 2(3^2)+1+2(3^{-1})+1(3^{-3}) = \mathbf{19.7037037037_{10}}$

Shashank Karthikeyan
A50703012

6. Remainder in parenthesis
    a. 4667/2 = 2333(1)/2 =1166(1)/2 = 583(0)/2 = 291(1)/2 = 145(1)/2 = 72(1)/2 = 36(0)/2 = 18(0)/2 = 9(0)/2 = 4(1)/2 = 2(0)/2 = 1(0)/2 = 0(1)
    → **00000000 00000000 00010010 00111011**
    b. (Binary conversion same as part a) → **10000000 00000000 00010010 00111011**
    c. 00000000 00000000 00010010 00111011
    → 11111111 11111111 11101101 11000100+1 =
    11111111 11111111 11101101 11000101