

---

## Homework 9 – Due Thursday, November 12, 2009 before the lecture

Please refer to the general information handout for the full homework policy and options. This homework contains 3 problems worth 10 points each. *Your solution to each problem should be handed in on a separate sheet of paper.*

**Reminder** Collaboration is permitted, but you must write the solutions *by yourself without assistance*, and be ready to explain them orally to the instructor if asked. You must also identify your collaborators. Getting solutions from outside sources such as the Web or students not enrolled in the class is strictly forbidden.

**Problems** Please practice on exercises and solved problems in Chapter 7. The material they cover may appear on exams.

1. (**Asymptotic notation**) For each of the following, answer *true* or *false*. No justification is required.

(a)  $2^{10} = O(n)$

(k)  $2^n = o(3^n)$

(b)  $16n = O(n)$

(l)  $1 = o(n)$

(c)  $n^4 = O(n^2 \log n)$

(m)  $2 \log n = o(\log n)$

(d)  $n \log n + 10n = O(n^2)$

(n)  $\frac{1}{3} = o(1)$

(e)  $3^n = O(2^n)$

(o)  $\log_2 n = \Theta(\log_3 n)$

(f)  $3^n = 2^{O(n)}$

(p)  $2^n = \Theta(4^n)$

(g)  $2^{2^n} = O(2^{2n})$

(q)  $n^5 = \Theta(32^{\log_2 n})$

(h)  $n^n = O(n!)$

(r)  $n^3 = \Omega(n^3)$

(i)  $n = o(n)$

(s)  $\log n = \Omega(\log(\log n))$

(j)  $2n = o(n^2)$

(t)  $2^{5^n} = \Omega(5^{2^n})$

2. (**Exponentiation cipher**) An exponentiation cipher encodes a message  $A$  using a ciphertext  $C = A^e \pmod{p}$  where  $p$  is a prime number and  $e$  is an integer exponent. (Here  $A$  and  $C$  are also integers.) You are given integers  $A, C, e$  and  $p$ , and you would like to determine whether  $C$  is a valid ciphertext for message  $A$ .

(a) Formulate this problem as a language  $EC$ .

(b) Explain why the following algorithm for  $EC$  does not run in polynomial time: *Compute  $A^e$  using  $e - 1$  multiplications. Take the result modulo  $p$  using one integer division, and compare the answer to  $C$ .*

(c) Show that  $EC \in P$ . *Hint:* First solve it when  $e$  is a power of 2.

3. (**Closure properties of P**) Prove that P is closed under

(a) (**2 points**) concatenation

(b) (**8 points**) star (*Hint:* Use dynamic programming. On input  $y = y_1 \cdots y_n$  for  $y_i \in \Sigma$ , build a table indicating for each  $i \leq j$  whether the substring  $y_i \cdots y_j \in A^*$  for any  $A \in P$ .)

Think about union and complement on your own.