Indian Institute of Information Technology, Vadodara

Course - Algorithms
Course Code - CS207
Prof. G Garg

EndSem

---

1. Give a tight asymptotic upper bound (O notations) on the solution to each of the following recurrences.

   a) $T(n) = 2T(\frac{n}{8}) + n^{\frac{ffl}{3}}$
   b) $T(n) = T(\frac{9n}{10}) + n$
   c) $T(n) = 3T(\frac{n}{2}) + n \log n$
   d) $T(n) = 4T(\frac{n}{2}) + n^2\sqrt{n}$
   e) $T(n) = T(\frac{n}{2}) + T(\frac{n}{4}) + T(\frac{n}{8}) + n$

2. An array $A[1 \ldots (2n+1)]$ is **wiggly** if $A[1] \leq A[2] \geq A[3] \leq A[4] \geq \ldots \leq A[2n] \geq A[2n+1]$. Given an unsorted array $B[1 \ldots (2n+1)]$ of real numbers, **design** and **analyse** an efficient algorithm that outputs a permutation $A[1 \ldots (2n+1)]$ of B such that A is a wiggly array.

3. Consider the RSA crypto system. Let $p = 11$ and $q = 13$.

   a) Compute n and $\phi(n)$
   b) Let the public key $e = 7$. Compute the private key d.
   c) Let the message that you want to send is $m = 2$. What is the encryption code c?
   d) Decrypt the c that you got above. Show all the steps.

4. Consider the **Diffie-Hellman** key exchange as discussed in the class. Let the common modulus be $p = 31$ and let the common ase $\alpha = 3$. Let the two parties be **Dilip** and **Aruna**. Let the private key of **Dilip** e $a = 7$ and let the private key of **Aruna** be $b = 11$.

   a) What does **Dilip** send to **Aruna**?
   b) What does **Aruna** send to **Dilip**?
   c) What is the common shared secret?

5. A general had 1200 soldiers at the start of a battle. After the battle, 3 soldiers were left over when they were lined up 5 at a time, 3 soldiers were left over when they were lined up 6 at a time, 1 soldier was left over when they were lined up 7 at a time, and no soldier was left over when they were lined up 11 at a time. How many soldier(s) survived the battle? Show all the steps.

```
while(noSuccess){
      tryAgain();
     if(Dead){
          break;
      }
}
```

Success Algorithm

Answers