

TENTAMEN T2 - 15 jan. 2007 - 10u30-12u30 - Zaal e0003

- Het tentamen is *gesloten boek*. Alle sommen tellen even zwaar.
- Zet op elk vel je gegevens.
- Voor *schakelcursisten*: opg. 1 en 2; tijd tot 11u30. Vermeld s.v.p. "*Schakelregeling*".
- *Licht steeds je oplossing toe* (dwz. laat zien dat je de theorie, methoden, trucs etc. kent). Veel succes!

1. a. Demonstreer hoe je volgens het algoritme van het dictaat een opspannende boom maakt in de complete graph op 5 punten. Zelfde vraag voor een Eulercircuit in de complete graph op 6 punten.

b. Los op: $T(n) = 3T(\frac{n}{3}) - 2$; $T(1) = 249$. Neem hierin voor n een macht van 3.

2. (Het zgn. "*Bottleneck TSP*"). Gegeven een graph G met een kostenfunctie (waarden $\in \mathbb{N}$) op de edges; alsmede een grens $b \in \mathbb{N}$. Bestaat er een Hamiltoncykel in G zodanig dat *elke* edge op die cykel gewicht $\leq b$ heeft? Gevraagd, dit probleem *NP-Compleet* te bewijzen volgens de behandelde standaardstappen.

3. a. Leg kort uit wat het verschil is tussen sorteeralgorithmen met plaatsinformatie of via comparisons; en sequentieel of parallel. Noem van elke categorie een voorbeeld.

b. Sorteert de volgende heap volgens de heapsort-methode: [17, 12, 10, 11, 6, 7, 9, 2, 3, 5].

4. a. Waarom is discrete log - encryptie "*snel*"?

b. In zeker Knapzak-cryptosysteem is de versluierde knapzakvector \underline{a} gelijk aan (17, 9, 27, 39). Verdere parameters zijn $w = 17$, $m = 42$ (zoals je weet is $\underline{a} = w \cdot \underline{a}' \bmod m$, met \underline{a}' superstijgend). Het cryptogram is 2. Gevraagd, de oorspronkelijke boodschap.