MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (From expected to strict running time). *Let $\mathcal{A}$ be an algorithm that always provides a solution to a puzzle and is guaranteed to have expected running-time τ and we need to construct a t-time algorithm that fails with low probability. One way to solve this is to stop the original algorithm $\mathcal{A}$ after s time steps. Let $\mathcal{A}_s$ be the corresponding algorithm which returns $\perp$ if $\mathcal{A}$ does not stop in s time steps and whatever $\mathcal{A}$ returns otherwise. Let $\mathcal{B}$ be the algorithm that runs $\mathcal{A}_s$ up to $\lfloor t/s \rfloor$ times to get the correct answer. Use Markov inequality to estimate the failure probability of $\mathcal{B}$. What is the minimal failure probability δ for fixed time-bound t? What is the minimal time-bound t to achieve failure probability δ. Graph the region of feasible solutions on $t\delta$-plane.*

Solution. W.l.o.g. We can assume that the algorithm $\mathcal{A}$ realises the Markov bound. If not we can modify the algorithm $\mathcal{A}$ such way that if it succeeds earlier it does empty computations until the time-bound s is reached and only then returns the answer.