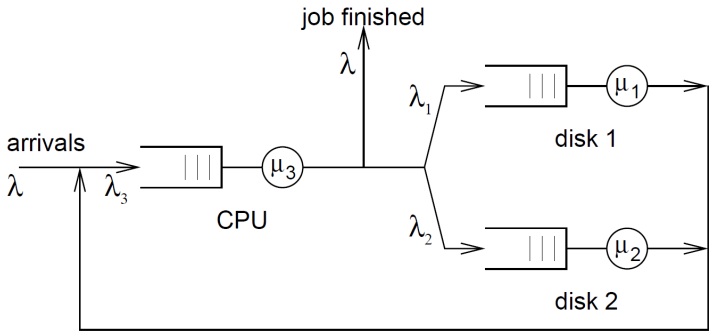
Solution to Task 11.1 (M/M/1-Queue)

a) Transition probabilities after leaving the CPU:

CPU $\rightarrow$ job finished: 1%
CPU $\rightarrow$ hard disk 1: 33%
CPU $\rightarrow$ hard disk 2: 66%

b) Arrival rates and loads:



As many jobs must leave the system as arrive from outside. From a) we know that only one percent of jobs leaving the CPU are finished. Therefore the arrival rate of the CPU must be 100 times the arrival rate from outside:

$$\lambda_3 = \frac{\lambda}{0.01} = \frac{0.3s^{-1}}{0.01} = 30s^{-1}$$

We also know that for 1 job leaving 33 enter disk 1, thus

$$\lambda_1 = 33 \cdot \lambda = 33 \cdot 0.3s^{-1} = 9.9s^{-1} \ ,$$

and 66 enter disk 2

$$\lambda_2 = 66 \cdot \lambda = 66 \cdot 0.3s^{-1} = 19.8s^{-1}$$

The loads ϱ_i:

$$\varrho_1 = \frac{\lambda_1}{\mu_1} = \frac{9.9s^{-1}}{20s^{-1}} = 0.495$$

$$\varrho_2 = \frac{\lambda_2}{\mu_2} = \frac{19.8s^{-1}}{25s^{-1}} = 0.792$$

$$\varrho_3 = \frac{\lambda_3}{\mu_3} = \frac{30s^{-1}}{200s^{-1}} = 0.15$$

c) The maximum value of λ:

Since $\varrho_2 > \varrho_1 > \varrho_3$, the queue of disk 2 is critical. To avoid an overload of the system, ϱ_2 must be less than 1:

$$\varrho_2 < 1 \quad \Leftrightarrow \quad \lambda_2 < \mu_2 = 25s^{-1}$$
$$\Rightarrow \lambda = \frac{\lambda_2}{66} < 0.379s^{-1}$$

d) Average processing time of a job:

All queues are of type M/M/1, thus the average processing times of the queues are denoted by

$$T_i = \frac{1}{\mu_i - \lambda_i}$$

We obtain for the queues:

$$T_1 = 99\text{ms};\ T_2 = 192\text{ms};\ T_3 = 5.88\text{ms};$$

The average processing time of a job is:

$$T_{\text{tot}} = 100 \cdot T_3 \ + \ 33 \cdot T_1 \ + \ 66 \cdot T_2 = 16.5s$$

e) Average number of jobs in the system:

With Little's theorem:

$$N_{\text{tot}} = \lambda T_{\text{tot}} = 0.3s^{-1} \cdot 16.5s = 4.96$$

f) The load on disk 2 is the highest, thus the performance of this disk has to be improved in order to reduce the average time of a job in the system. With doubling the service rate of disk 2, $\mu_2^{'} = 50s^{-1}$, and

$$\begin{aligned}
\varrho_2^{'} &= \frac{\lambda_2}{\mu_2^{'}} = \frac{19.8}{50} = 0.396\ , \\
T_2^{'} &= \frac{1}{\mu_2^{'} - \lambda_2} = \frac{1}{50 - 19.8} = 33\text{ms}\ , \\
T_{\text{tot}}^{'} &= 100 \cdot T_3 \ + \ 33 \cdot T_1 \ + \ 66 \cdot T_2^{'} = 6.03s\ , \\
N_{\text{tot}}^{'} &= \lambda \cdot T_{\text{tot}}^{'} = 1.81\ .
\end{aligned}$$

Solution to Task 11.2 (Symmetric Cryptosystems and Perfect Security)

a) Let $c = E(m,k)$ and $c' = E(m',k)$ for some $k \in \mathcal{K}$ and $m, m' \in \mathcal{M}$. We have to show that $c = c'$ implies $m = m'$.

Let $c = c'$. Then the following holds:

$$m = D(E(m,k),k) = D(c,k) \overset{!}{=} D(c',k) = D(E(m',k),k) = m.$$

Hence, E is injective in its first argument.

b) We know that $H(C|M,K) = 0$ because c can be calculated by $c = E(m,k)$ and $H(M|C,K) = 0$ because m can be determined by decrypting c using the key k.

With this, we obtain

$$H(M,K,C) = H(M,K) + \underbrace{H(C|M,K)}_{=0} = H(M,K) \underset{M,K\text{independent}}{=} H(M) + H(K) \tag{1}$$

and

$$H(M,K,C) = H(K,C) + \underbrace{H(M|K,C)}_{=0} = H(K,C). \tag{2}$$

Using the definition of the conditional entropy, we get:

$$H(K|C) = H(K,C) - H(C) \underset{(2)}{=} H(M,K,C) - H(C) \underset{(1)}{=} H(M) + H(K) - H(C)$$

c) We know that

$$\begin{aligned} H(M|C) + H(K|M,C) &= H(M,C) - H(C) + H(K|M,C) \\ &= H(K,M,C) - H(C) \\ &= H(M|K,C) + H(K,C) - H(C) \end{aligned}$$

Since the message m can be uniquely reconstructed from k and c by the decryption algorithm, it holds that $H(M|K,C) = 0$. Therefore,

$$H(M|C) + H(K|M,C) = H(K,C) - H(C) = H(K|C)$$

d) We can prove the first inequality without the assumption that the cryptosystem is perfectly secure:

$$H(M) \underset{b)}{=} H(K|C) - H(K) + H(C) \underset{H(K|C)\leq H(K)}{\leq} H(C) \tag{3}$$

We also know that

$$H(K) + H(M) - H(C) \underset{b)}{=} H(K|C) \underset{c)}{=} H(M|C) + H(K|M,C)$$

Using the perfect security property $H(M) = H(M|C)$, we obtain

$$\begin{aligned} H(K) + H(M) - H(C) &= H(M) + H(K|M,C) \\ \Leftrightarrow H(K) &= H(C) + \underbrace{H(K|M,C)}_{\geq 0} \geq H(C) \end{aligned} \tag{4}$$

Thus,

$$H(M) \underset{(3)}{\leq} H(C) \underset{(4)}{\leq} H(K)$$