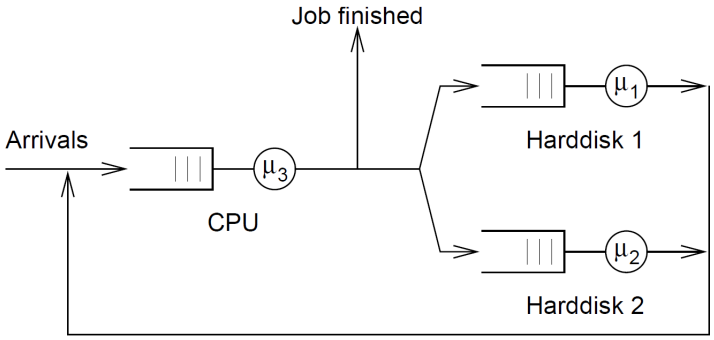
Task 10.1 (M/M/1-Queue)

A computer system for stack processing consists of a central processing unit (CPU) and 2 harddisks. Arriving jobs are at first processed by the CPU. Then they can leave the system or address one of the harddisks. In the latter case, the job reenters the CPU.



The system shall be modelled as a lossless exponential network. From measurements we know that on average $\lambda = 0.3\,\text{jobs/s}$ enter the CPU from outside. On average, each job visits harddisk 1 for 33 times and harddisk 2 for 66 times before leaving the system. The service rates are: $\mu_3 = 200\,\text{jobs/s}$ for the CPU, $\mu_1 = 20\,\text{jobs/s}$ for harddisk 1 and $\mu_2 = 25\,\text{jobs/s}$ for harddisk 2.

a) Determine the transition probabilities after leaving the CPU.

b) What are the arrival rates λ_i and the loads ϱ_i for the individual queues?

c) What is the maximum value of λ for which the system is **not** overloaded?

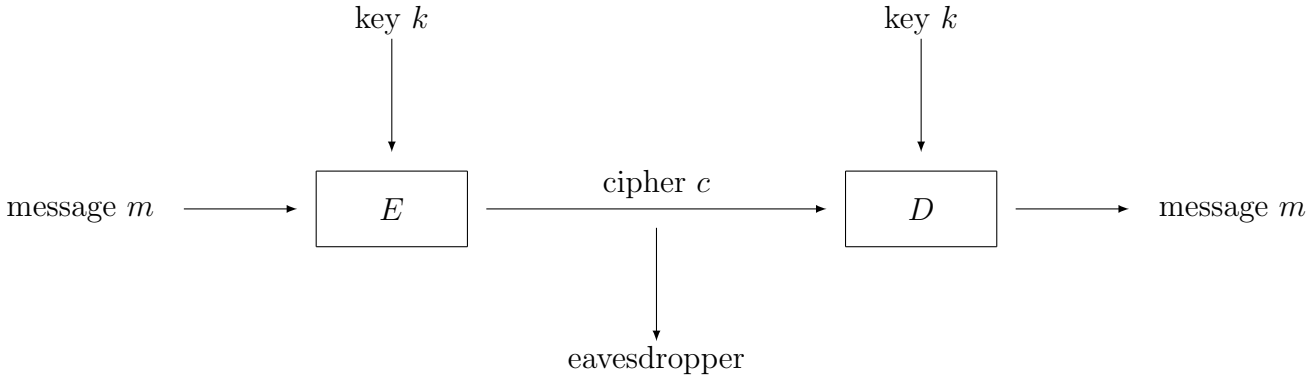
d) What is the average processing time of a job?

e) How many jobs are in the system on average?

f) The performance of which component should be improved to reduce the average time of a job in the system? What is the effect of doubling the service rate of this component?

Task 10.2 (Symmetric Cryptosystems and Perfect Security)

A *symmetric cryptosystem* is a pair of an *encryption* (E) and a *decryption* (D) function using the same key k, which is assumed to be known by both E and D (symmetry)[1]. In the model, an *eavesdropper* only has access to the *cipher*.



Let $\mathcal{K}$ be the set of all possible keys, $\mathcal{M}$ the set of messages and $\mathcal{C}$ the set of all ciphers. Then E and D are functions

$$\begin{aligned} E: &\quad \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C} \\ D: &\quad \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M} \end{aligned}$$

such that $D(E(m,k),k) = m$ for all $m \in \mathcal{M}$ and $k \in \mathcal{K}$.

a) Show that E is an injective mapping in its first argument.

We now assume that m and k are chosen independently at random from $\mathcal{M}$ and $\mathcal{K}$. Hence, we can define the random variables M, K and C corresponding to m, k and c. Prove the following two statements

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

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

A cryptosystem is called *perfectly secure*, if $H(M) = H(M|C)$, i.e., an eavesdropper does not gain more knowledge about the message by eavesdropping the cipher.

d) Show that every perfectly secure cryptosystem satisfies $H(M) \leq H(C) \leq H(K)$.

[1] The method how k is exchanged is not part of the mathematical model of the cryptosystem. Hence, it is not applicable to secure communication between users that do not have the possibility to securely exchange the key. This is the reason why most used cryptosystems today are *public-key cryptosystems*.