

Reading: Rosen edition 5: Sections 4.1–4.6 and 5.1–2, or edition 4: Sections 4.1–4.6.

(1) How many ways are there to order the letters of the word “INDISCREETNESS”. Give a brief explanation for your answer.

(2) Consider a distributed system with n processors. In monitoring the system, we will have each of the n processors in one of 3 states: “running”, “waiting” or “done”. There can be many processes running at the same time. We say that the system is *blocked* if some process is waiting while no process is running. How many non-blocked configurations are there? Give a brief explanation for your answer.

(3) Multiple senders are each sending a stream of packets across one channel. The link multiplexes the streams by interleaving the two sequences. For example if there are two senders, sender A sending sequence a_1, a_2, a_3 and sender B sending b_1, b_2 , then the multiplexed sequence will have length 5, consisting of the 5 packets above, such that the a packets arriving in order, and the b packets also arrive in order, but they can be intermixed in any order. Examples of the multiplexed stream include a_1, a_2, b_1, a_3, b_2 or b_1, a_1, a_2, a_3, b_2 etc., but the sequence a_1, a_3, b_1, a_2, b_2 is not an acceptable multiplexed stream, as a_2 arrived before a_3 .

- (a) If two senders multiplex streams with n and m packets respectively, what is the number of possible multiplexed streams. Give a formula in terms of n and m .
- (b) If three senders multiplex streams with n , m and k packets respectively, what is the number of possible multiplexed streams. Give a formula in terms of n , m , and k .

For each case, briefly explain why your answer is correct.

(4) A standard way to achieve increased security is to use multiple passwords. Of course, if everyone knows all the passwords then there is little advantage of using many. However, in some high importance systems (e.g, those controlling rockets), no one person is supposed to be able to control the system. There will be a set of n guards whose job is to control this system together. One way to achieve this is to give each of the n guards a different password, and require all n passwords to control the system. However, this causes trouble if one of the n guards cannot be found. In this problem, you will design a fail-safe system with n guards that satisfies the following two rules:

- any subset of $k \leq n/2$ guards should not be able to login and control the system
- any subset of $k > n/2$ is able to login and control the system.

To achieve this you will give each guard i a set X_i of passwords. Let $S = \cup_i X_i$ be the set of all passwords. Now any subset A of guards can log in, if they have all the passwords, that is if $\cup_{i \in A} X_i = S$. Design a fail-safe system for 5 guards with as few passwords as possible. This means two things, design a fail-safe system for 5 guards with k passwords for some k , and prove that all fail-safe systems with 5 guards must use at least k passwords.

(5) You select a random integer between 1 and $35n$ for some integer n each integer in this range equally likely. What is the probability that your selected number is divisible by 5 or 7? Briefly explain your answer: what is the sample space, probability, and the event in question.

(6) You throw k dice independently (each can land on aside with the number 1, 2, 3, 4, 5, or 6 written).

- (a) What is the probability that the first die is 1?
- (b) What is the probability that the first dice is 1 conditioned that the first two dice sums to 7?
- (c) What is the probability that the first dice is 1 conditioned that the first three dice sums to 8?

For each part briefly explain your answer: what is the sample space, probability, and the event in question.

(7 optional) In the last problem set we considered quorum systems, and designed system with as many sets as possible. An important attribute of quorum systems is *availability*. Here is what we mean by availability. Assume that the quorum system \mathcal{Q} is on a set of n processors, and each of the n processors can fail with probability p independently. We assume that failure is crash failure, if a machine failed that will be obvious for all observers. The availability of a quorum system is the probability that for one of the sets $A \in \mathcal{Q}$ no element of A failed.

- (a) Give a formula for the availability of the quorum system we used for problem 6 in the previous problem set in terms of p and n . Briefly explain your answer: what is the sample space, probability, and the event in question.
- (b) Assume n is odd and let $n = 2k + 1$. An alternate quorum system would be to let \mathcal{Q} be all subsets of size $k + 1$. Give a formula for the size of this quorum system n (or k). Assume $p = .5$. Give a formula for the availability of this quorum system as a function of n or k . Briefly explain your answer: what is the sample space, probability, and the event in question.