

F. Autreau
P. Lafourcade
JL. Roch

P. Lafourcade.

SET 1

Date: 20.09.2007

Exercise 1

Give the security properties that an international airport should guarantee.

Exercise 2

Suppose a certain drug test is 99% accurate, that is, the test will correctly identify a drug user as testing positive 99% of the time, and will correctly identify a non-user as testing negative 99% of the time. Let's assume a corporation decides to test its employees for opium use, and 0.5% of the employees use the drug.

We want to know the probability that, given a positive drug test, an employee is actually a drug user.

Exercise 3

Prove that for real random variables X and Y , and real number a , we have $E[X + Y] = E[X] + E[Y]$ and $E[aX] = aE[X]$. And if X and Y are independent real random variables, then $E[XY] = E[X]E[Y]$

Exercise 4

Let X be a real random variable, and let a and b be real numbers. Then we have:

$$(i) \text{Var}[X] = E[X^2] - (E[X])^2$$

$$(ii) \text{Var}[aX] = a^2 \text{Var}[X]$$

$$(iii) \text{Var}[X + b] = \text{Var}[X]$$

Exercise 5

Prove Markov's inequality: Let X be a random variable that takes only non-negative real values. Then for any $t > 0$, we have

$$P[X \geq t] \leq \frac{E[X]}{t}$$

Exercise 6

Prove Chebyshev's inequality: Let X be a real random variable. Then for any $t > 0$, we have:

$$P[|X - E[X]| \geq t] \leq \frac{\text{Var}[X]}{t^2}$$

Exercise 7

Prove Chernoff bound: Let X_1, \dots, X_n be mutually independent random variables, such that each X_i is 1 with probability p and 0 with probability $q := 1 - p$. Assume that $0 < p < 1$. Also, let \bar{X} be the sample mean of X_1, \dots, X_n . Then for any $\epsilon > 0$, we have:

$$\begin{aligned} (i) P[\bar{X} - p \geq \epsilon] &\leq e^{-n\epsilon^2/2q} \\ (ii) P[\bar{X} - p \leq -\epsilon] &\leq e^{-n\epsilon^2/2p} \\ (iii) P[|\bar{X} - p| \geq \epsilon] &\leq 2e^{-n\epsilon^2/2} \end{aligned}$$

Exercise 8

Generalization of Birthday Paradox:

The setting is that we have q balls. View them as numbered, $1, \dots, q$. We also have N bins, where $N \geq q$. We throw the balls at random into the bins, one by one, beginning with ball 1. At random means that each ball is equally likely to land in any of the N bins, and the probabilities for all the balls are independent. A collision is said to occur if some bin ends up containing at least two balls. We are interested in $C(N, q)$, the probability of a collision. The birthday paradox is the case where $N = 365$. We are asking what is the chance that, in a group of q people, there are two people with the same birthday, assuming birthdays are randomly and independently distributed over the days of the year.

Let $C(N, q)$ denote the probability of at least one collision when we throw $q \geq 1$ balls at random into $N \geq q$ buckets. Then

$$\begin{aligned} C(N, q) &\leq \frac{q(q-1)}{2N} \\ C(N, q) &\geq 1 - e^{q(q-1)/2N} \end{aligned}$$

Also if $1 \leq q \leq \sqrt{2N}$ then $C(N, q) \geq 0 : 3 \cdot \frac{q(q-1)}{N}$. Hint: first prove the inequality $(1 - 1/e) \cdot x \leq 1 - e^{-x} \leq x$

Exercise 9

Message are composed of $\{0, 1\}$, keys are $\{A, B\}$ and we know $P(0) = 1/4, P(1) = 3/4, P(A) = 1/4, P(B) = 3/4$. The encryption is defined by:

$$E_A(0) = a, E_A(1) = b, E_B(0) = b, E_B(1) = a$$

This encryption is it perfectly secure?

Exercise 10

Prove or disprove:

- The function $f(n) := (\frac{1}{2})^n$ is negligible.
- The function $f(n) := 2^{-\sqrt{n}}$ is negligible.
- The function $f(n) := n^{-\log n}$ is negligible.

Exercise 11

Prove or disprove the following statements:

1. If both $f, g \geq 0$ are noticeable, then $f - g$ and $f + g$ are noticeable.
2. If both $f, g \geq 0$ are not noticeable, then $f.g$ is not noticeable.
3. If both $f, g \geq 0$ are not noticeable, then $f + g$ is not noticeable.
4. If $f \geq 0$ is noticeable, and $g \geq 0$ is negligible, then $f.g$ is negligible.
5. If both $f, g > 0$ are negligible, then f/g is noticeable.