Prerequisites Test

Cryptography and Security 2025

Name: _____

SCIPER: _____

- This document contains **3** independent exercises.
- **Do NOT open this document until the beginning of the exam**.
- Duration: **105 minutes** (one hour and forty-five minutes).
- **This is a closed book exam. No extra sheet is allowed**.
- Allowed Material: blue or black pen (avoid pencils), eraser. Any kind of electronic device is forbidden.
- Food and water are allowed but should not disturb the exam when consumed.
- Blank pages are provided at the end of the exam and can be used as scrap paper or to report answers. If needed, additional scrap paper will be provided.
- **Only answers directly written on the exam sheet will be corrected**.
- Each answer must be written in English in the dedicated box. If the answer is put at the end, **clearly** indicate which exercise it refers to. In particular, properly separate scrap text from answers to be corrected.
- Non-trivial statements must be **cleanly and formally justified**.
- Questions about the (technical) content of the exam will not be answered.
- **Prepare the CAMIPRO card or an official ID paper for the identity check**.

Exercise 1 Algorithm: Constructing a Suspended Bridge

One day, a friend calls you for help: he needs to build a suspended bridge of length $n-1$ meters inside a deep cavern, but the construction rules leave him perplex. You are given an unlimited supply of identical steel bars, each exactly 1 meter long:

1. At both ends of the bridge, and at every intermediate meter, the bridge must be welded to a steel bar.
2. Bars can only be welded at their extremities (called *welding points*), and only at an angle $\pi/6$ from the vertical.
3. There is a unique *anchor point* located at $\frac{\sqrt{3}}{2}n$ meters from the bridge's base. It must be used, supports at most two bars, and serves as the root of the suspension.
4. For all *welding points*, we must have an *ascending path* (steel bar connecting the point to the anchor point without ever going down).
5. The entire structure must fit inside an equilateral triangle of side length $n-1$.

Fig. 1 gives an example of a valid construction.

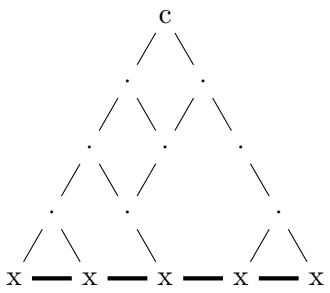


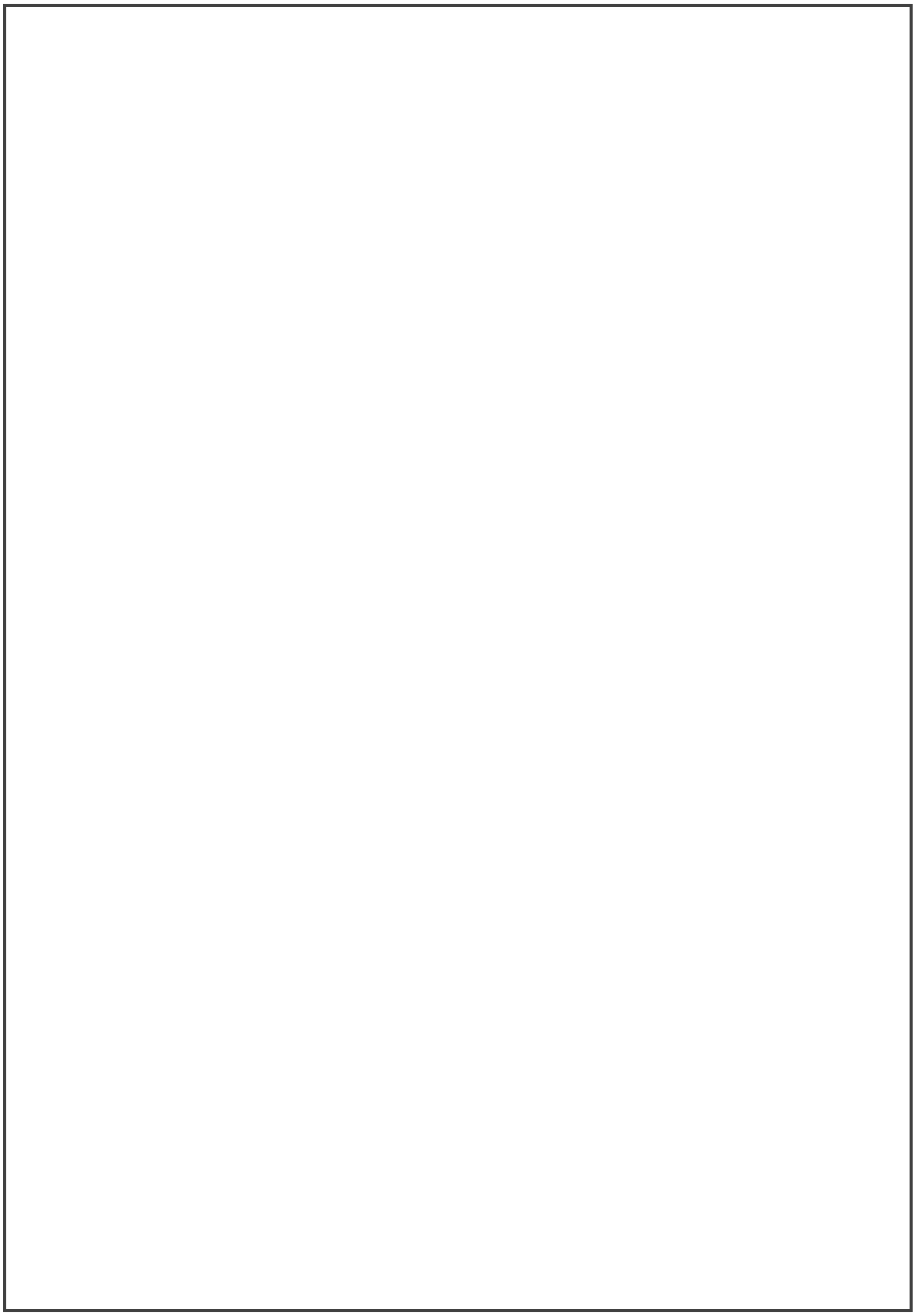
Figure 1: A valid suspended bridge of 4 meters. It cost 15 steel bars.

Your task is to construct such a bridge with *minimal cost*, where the cost is defined as the number of steel bars used.

Question 1.1

Show that any valid construction containing a cycle cannot minimize the cost.

Hint: Consider defining the ascending distance *of a welding point as the shortest length of an ascending path connecting it to the anchor point.*



Question 1.2

Using the fact that an optimal solution has to be a *rooted binary tree*, let $C(n)$ denote the minimal cost for a bridge of length $n-1$. Find a formula to compute $C(n)$ and show that $C(n) = O(n \log n)$. *Hint: for the asymptotic analysis, you may assume that n is a power of two.*

Question 1.3

Design an algorithm that computes $C(n)$ for any $n > 0$. Your algorithm should run in $O(n^2)$ time and $O(n)$ memory for full points.

Exercise 2 Probability: Are Random Walks Recurrent ?

In this exercise, we explore whether random walks are *recurrent* (i.e., they almost surely return to the origin infinitely often) or not.

Let $(S_n)_{n\geq 0}$ be the simple symmetric random walk on $\mathbb{Z}$ starting at 0:

$$S_n = \sum_{i=1}^{n} X_i, \qquad X_i \overset{\text{iid}}{\sim} \begin{cases} +1 & \text{with prob. } \frac{1}{2}, \\ -1 & \text{with prob. } \frac{1}{2}. \end{cases}$$

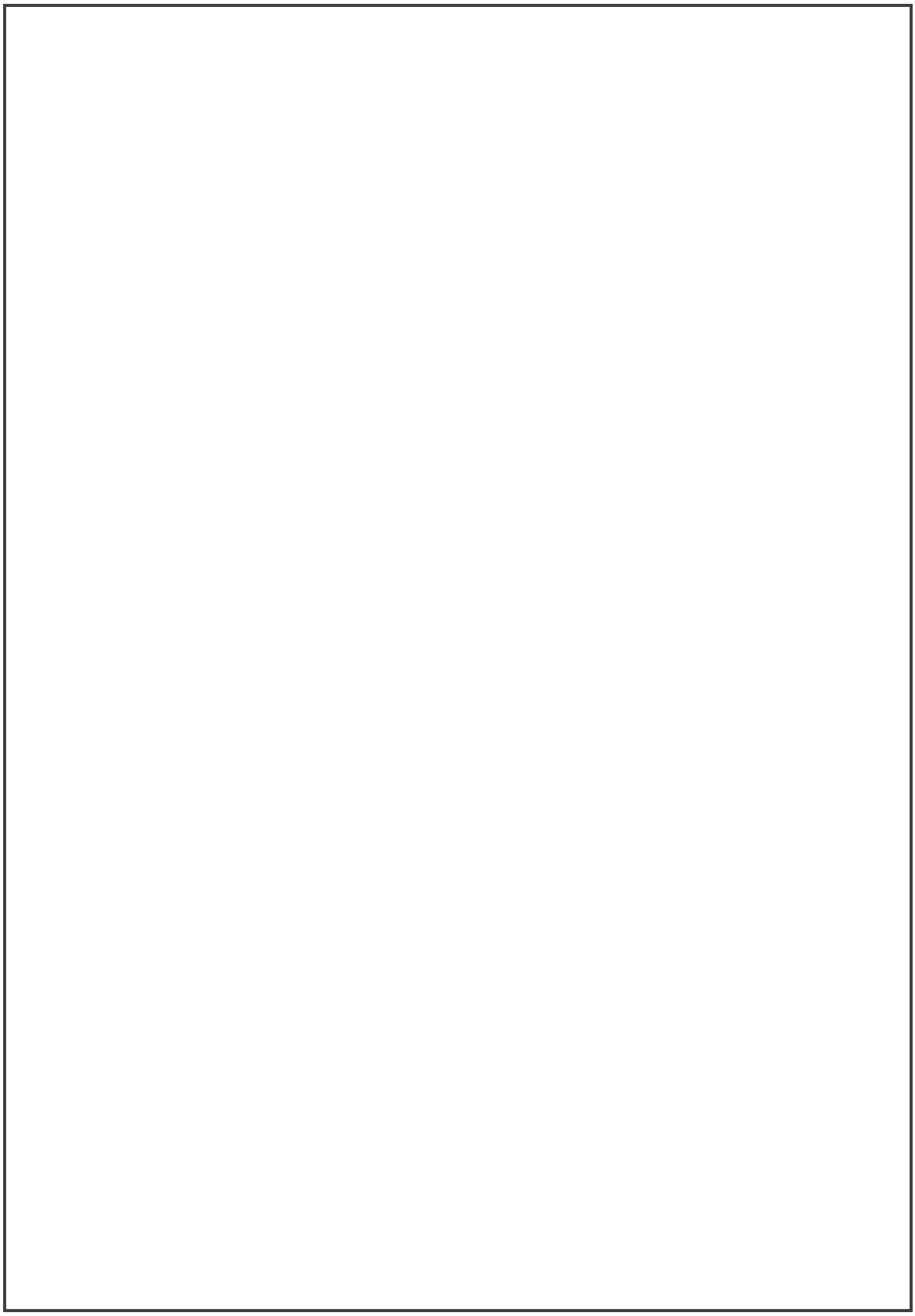
Define the random variable $V := \sum_{n=1}^{\infty} \mathbf{1}_{\{S_n=0\}}$ the total number of returns to the origin (excluding time 0), and set $\rho := \mathbb{P}[V \geq 1]$.

Question 2.1

Prove that $\mathbb{E}[V] = \frac{\rho}{1-\rho}$. Deduce that

$$\begin{cases} \sum_{n=1}^{\infty} \mathbb{P}[S_n = 0] = \infty & \implies \quad \rho = 1, \\ \sum_{n=1}^{\infty} \mathbb{P}[S_n = 0] < \infty & \implies \quad \rho < 1. \end{cases} \tag{1}$$

Hint: You can use the fact that $\mathbb{P}[V \geq k] = \rho^k$.



Question 2.2

Give a closed formula for $\mathbb{P}[S_m = 0]$ and use an approximation to show that $\rho = 1$.

Hint: Remember Stirling's formula: $n! \simeq \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$.

Question 2.3

Assuming eq. (1) generalises to higher dimension (it does), generalize the previous result to any dimension, i.e. $\mathbb{Z}^g$, for $g = 2, 3, 4, \cdots$. That is, determine what is ρ for a random walk in g-dimension S_n^g, where $S_n^g = \sum_{i=1}^n (X_{i,1}, \cdots, X_{i,g})$ and each $X_i \in \mathbb{Z}^g$ is i.i.d. with uniform step distribution.

Example 1. For $g = 2$, $S_n^2 = \sum_{i=1}^n Y_i$ where $Y_i \overset{iid}{\sim} Y = \begin{cases} (1,1) & \text{w.p. } 1/4 \\ (-1,1) & \text{w.p. } 1/4 \\ (1,1) & \text{w.p. } 1/4 \\ (1,-1) & \text{w.p. } 1/4 \end{cases}$

Exercise 3 Number Theory: Wilson's Theorem and Wolstenholme's Theorem

Let $p > 5$ be a prime number.

Question 3.1

Let p be a prime number. Prove that $(p-1)! \equiv p-1 \pmod{p}$.

Hint: For any $1 \leq x < p$, what is the solution y such that $x \cdot y = 1 \bmod p$?

Question 3.2

Let $1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b}$ for some positive integers a and b and $\gcd(a, b) = 1$. Show that $p \mid a$.
Hint: $p \mid a \iff p \mid (p-1)! \cdot a \iff p \mid (p-1)! \cdot \frac{a}{b}$.

Question 3.3

Following the previous question, show that $p^2 \mid a$.

Hint: $\sum_{i=1}^{p-1} i^2 = \frac{p(p-1)(2p-1)}{6}$.