



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE  
ESCUELA DE INGENIERÍA  
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

**Criptografía y Seguridad Computacional - IIC3253**  
**1<sup>er</sup> semestre - 2022**  
**Lothar Droppelmann**

## **Ayudantía 3**

### **Parte 1**

Paradoja de los cumpleaños. Calcule el menor  $k \in N$  posible tal que la probabilidad de que, al elegir  $k$  elementos con repetición de un grupo de  $n$  elementos, se elijan 2 o más iguales, sea mayor o igual a  $\frac{1}{2}$ .

### **Parte 2**

Merkle Tree. Explicación de como funciona un Merkle Tree y cuales son sus usos y propiedades.