Pontificia Universidad Católica de Chile
Departamento de ciencias de la computacion
IIC3253 – Criptografía y Seguridad Computacional
Primer Semestre del 2025

Ayudantía 09

RSA - Algoritmos de RSA

Ayudante: Manuel Cifuentes – mecifuentes@uc.cl

Repaso

Problema 1 (Exponenciacion Rapida)

Se le pide calcular 7^{23} mód 15.

1. Resolver 7^{23} mód 15 usando el método tradicional
2. Resolver 7^{23} mód 15 usando exponenciación rápida
3. ¿De qué nos sirve utilizar Exponenciación Rápida en Criptografía?

Problema 2 (RSA)

Realice una demostracion practica del algoritmo RSA, con $P = 19$ y $Q = 31$. para un mensaje $m = 121$

Problema 3 (Test Primalidad)

Sea $p(x)$ un polinomio de grado k, donde $k \geq 1$, $a_k \in \{1, \ldots, n-1\}$ y cada $a_j \in \{0, \ldots, n-1\}$ para $0 \leq j \leq k-1$.

Una raíz de $p(x)$ módulo n es un número a tal que

$$p(a) \equiv 0 \pmod{n}.$$

Demostrar que si n es un número primo, entonces $p(x)$ tiene a lo más k raíces en el conjunto $\{0, 1, \ldots, n-1\}$.