tema cryptografie

Avram Flavian

21 February 2026

1 Introduction

Calculați complexitatea funcției `a_la_b_mod_c` în raport cu lungimea parametrilor. Comparați cu exponențierea modulară obișnuită.

2 Tabelul principal

Table 1: Titlul tabelului

Element	Nr. repetări	Cost	Cost total
a % b = c	1	1	1
p = 1	1	1	1
`while b`	$\log_2 b$	1	$\log_2 b$
`if b % 2 == 1`	$\log_2 b$	1	$\log_2 b$
`p = (p*a)%c`	$\log_2 b/2$	nr1	$\text{nr1} \cdot \log_2 b/2$
`a = (a*a)%c`	$\log_2 b$	nr2	$\text{nr2} \cdot \log_2 b$
`b //= 2`	$\log_2 b$	1	$\log_2 b$
`return p`	1	1	1

$T(b) = 3 + 3\log_2 b + \frac{\text{nr1}}{2}\log_2 b + \text{nr2}\log_2 b$

$\log_2 b = n$

$T(b) = 3 + 3n + \frac{\text{nr1}}{2} \cdot n + \text{nr2} \cdot n$

$n =$ numărul de biți ai lui b

$m =$ numărul de biți ai lui a și c

$\text{nr1} = m^2$ (deoarece înmulțim p cu a)

$\text{nr2} = m^2$ (deoarece înmulțim a cu a)

$T(b) = 3 + 3n + \frac{m^2 n}{2} + m^2 n$

$T(b) \in O(n \cdot m^2)$

Exponentierea naivă: $b = 2^n \Rightarrow T_{\text{naiv}} \in O(2^n \cdot m^2)$