

# SaDS HW 7

Inti Mendoza

## Problem 7.1

See `rsa.cpp`

Due to numbers getting pretty big, choose small  $n$  (preferably single digit - I usually use 2) else you'll be waiting very long for results.

## Problem 7.2

Let  $x = (x_1, \dots, x_n)$  be a sequence s.t.  $h(x) = k$ . To find the collision select  $x' = (x'_1, \dots, x'_{n-1})$  and compute  $x'_n = (a_n^{-1} \cdot (k - \sum_{i=1}^{n-1} a_i x'_i))^{1234567} \bmod 9993201131$  where  $a_i$  are coefficients inside our given hashing function.

$\therefore$  we can obtain  $h(x) = h'(x) = k$  and find a collision. Since computational power is not there yet without complex libraries, I cannot obtain concrete results.

## Problem 7.3

See `hash.cpp`

Due to exploding huge numbers, your pc might not be able to produce results. I suggest just look at the code and see everything is gucci - good.

$hash(s)$	$s$
-----------	-----

empty table still a table

## Problem 7.4

Phrase: ayy lmao