Assignment 24

Alex Clemmer
Student number: u0458675

1

The expression `z = (z * x) mod N` occurs in $O(n^2)$. Since N is an n-bit number, and since x and y are strictly less than N, the worst possible case is that x and y both have a value of $2^n - 2$.

This means that the $O(n^2)$ statement, which easily dominates the inner part of the loop, gets iterated $2^n - 2$ times. That gives us:

$$O(2^n \cdot n^2) \tag{1}$$

Gross!

2

So `z = x * y` should be $O(n^2)$, depending on the algorithm you use. N is an n-bit number, which means its worst case value is $2^n - 1$, which means that the loop ends up iterating 2^n times asymptotically. The statement inside the loop is only slightly trickier: `z-N` is linear, and allocating the result into z is also linear. So either way, the loop takes $O(2^n)$, and the loop itself should take $O(n)$ time. So that gives us $O(n^2) + O(n \cdot 2^n)$, which is really just:

$$O(n \cdot 2^n) \tag{2}$$

Better, but still horrible.