$\mathbf{Judge}\ J$	Ir	$\mathbf{verter}\ I$
sample primes $p, q \in [2^k, 2^{k+1})$		
n := pq		
sample prime $e \in \mathbb{Z}_{\phi(n)}^*$		
sample $x \in \mathbb{Z}_n$		
$y := x^e$		
		J.n, J.e, J.y
. I	cc	ompute x
$ ightharpoonup I.x$ return $x \stackrel{?}{=} I.x$		
$\mathbf{return} \ x = 1.x$		