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