

Judge J

sample primes $p, q \in [2^k, 2^{k+1})$

$n := pq$

sample prime $e \in \mathbb{Z}_{\phi(n)}^*$

sample $x \in \mathbb{Z}_n$

$y := x^e$

► x'

return $x \stackrel{?}{=} x'$

Inverter I

► n, e, y
compute x'