Judge J	**Inverter** I	**virtual** A
sample primes $p, q \in [2^k, 2^{k+1})$ $n := pq$ sample prime $e \in \mathbb{Z}^*_{\phi(n)}$ sample $x \in \mathbb{Z}_n$ $y := x^e$		
	▶ $J.n, J.e, J.y$	
	▶ m°	select m°
	$b := J.y$ $e := J.e$ sample $\sigma^\circ \in \mathbb{Z}_n$ $a := b^{m^\circ}(\sigma^\circ)^e$ $pk := e \Vert a \Vert b$	
		▶ pk, σ° forge (m, σ)
	▶ (m, σ)	
	if $m^\circ < m$ **then** swap (m°, σ°) and (m, σ)	
	$f := m^\circ - m$ $\rho := \sigma / \sigma^\circ$	
	find $u, v \in \mathbb{Z} : ue + vf = 1$ $x := b^u \rho^v$	
▶ $I.x$ **return** $x \stackrel{?}{=} I.x$		