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 $x \in \mathbb{Z}_n$ $y := x^e$		
	▶ n, e, y	
	▶ $\widetilde{m}$	select $\widetilde{m}$
	$b := y$ sample $\widetilde{\sigma} \in \mathbb{Z}_n$ $a := b^{\widetilde{m}}\widetilde{\sigma}^e$ $pk := e \Vert a \Vert b$	
		▶ $pk, \widetilde{\sigma}$ forge (m, σ)
	▶ (m, σ)	
	if $\widetilde{m} < m$ **then** swap $(\widetilde{m}, \widetilde{\sigma})$ and (m, σ)	
	$f := \widetilde{m} - m$ $\rho := \sigma / \widetilde{\sigma}$	
	find $u, v \in \mathbb{Z} : ue + vf = 1$ $x' := b^u \rho^v$	
▶ x' **return** $x \stackrel{?}{=} x'$		