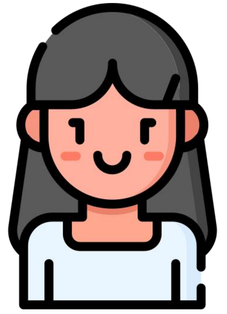
$\mathcal{P}$

1. Sample r from $\mathbf{Z}_N$ uniformly
2. Send $a = r^2 \pmod N$

$\mathcal{V}$



I know w s.t.
$w^2 = x \pmod N$

Is x indeed a quadr. residue?