$m \leftarrow \mathcal{M}_0$

pk

$\mathcal{M}_0$

$\mathsf{Enc}_{\mathsf{pk}}(m)$

Given

– pk

– $\mathcal{M}_0$

– $\mathsf{Enc}_{\mathsf{pk}}(m)$

Charlie tries to guess $g(m)$

$m \leftarrow \mathcal{M}_0$

pk

$\mathcal{M}_0$

Given

– pk

Charlie tries to guess $g(m)$