



pk

\mathcal{M}_0

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



Given

– pk

– \mathcal{M}_0

– $\text{Enc}_{pk}(m)$

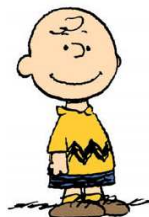
Charlie tries to guess $g(m)$

$m \leftarrow \mathcal{M}_0$



pk

\mathcal{M}_0



Given

– pk

Charlie tries to guess $g(m)$

$m \leftarrow \mathcal{M}_0$