

$c$ 

ciphertext: ISSIBIG...

 $k$ 

key: KEY---

 $P(k, c)$ 

plaintext: YOUKNOW...

input: KEY---ISSIBIG...

target: KEY---YOUKNOW...

