

~~EXAMPLE~~ EXAMPLE of KNOWN-PLAINTEXT ATTACK

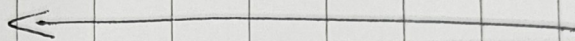
CAR

CAR KEY

(k)

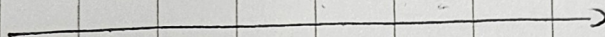
(k)

OPEN



$m \leftarrow \$ \text{ ~~car~~ } M$

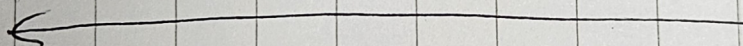
m



compute

$$c = \text{Enc}_k(m)$$

c



IF

$$c = \text{Enc}_k(m),$$

OPEN.

$\Rightarrow$ Adversary sees both m and c (hence, known-plaintext attack).

(Note that m changes every time!)