

# Crypto refresher

IND-CPA: Indistinguishability under Chosen Plaintext Attack

- **IND-CPA** is a game against an adversary  $\mathcal{A}$  having access to an oracle  $\mathcal{O}$ 
  1. Game chooses  $k \in \mathcal{K}$ ,  $b \in \mathbb{B}$  and  $m_0, m_1 \in \mathcal{P}$  and sends  $c \leftarrow \text{Enc}_k(m_b)$  to  $\mathcal{A}$
  2.  $\mathcal{A}$  gets  $c_i \leftarrow \text{Enc}_k(m_i)$  from  $\mathcal{O}$  for messages  $m_i \in \mathcal{P}$  of their choosing
  3.  $\mathcal{A}$  guesses  $b' \in \mathbb{B}$  and wins if and only if  $b = b'$
- A cryptosystem is **CPA secure** if no adversary wins this game more than half the time

# Crypto refresher

IND-CCA: Indistinguishability under Chosen Ciphertext Attack

- **IND-CCA** is a game against an adversary  $\mathcal{A}$  having access to an oracle  $\mathcal{O}$ 
  1. Game chooses  $k \in \mathcal{K}$ ,  $b \in \mathbb{B}$  and  $m_0, m_1 \in \mathcal{P}$  and sends  $c \leftarrow \text{Enc}_k(m_b)$  to  $\mathcal{A}$
  2.  $\mathcal{A}$  gets  $c_i \leftarrow \text{Enc}_k(m_i)$  from  $\mathcal{O}$  for messages  $m_i \in \mathcal{P}$  of their choosing
  3.  $\mathcal{A}$  gets  $\tilde{m}_i \leftarrow \text{Dec}_k(c_i)$  from  $\mathcal{O}$  for ciphertext  $c_i \in \mathcal{C}$  of their choosing (except  $c$ )
  4.  $\mathcal{A}$  guesses  $b' \in \mathbb{B}$  and wins if and only if  $b = b'$
- A cryptosystem is **CCA secure** if no adversary wins this game more than half the time