Crypto refresher

What's a cryptosystem

- A **cryptosystem** is a tuple Π with key, plaintext and ciphertext spaces $\mathscr{K}, \mathscr{P}, \mathscr{C}$

$$\Pi = \begin{cases} Gen : 1^n \to \mathscr{K} \\ Enc : \mathscr{K} \times \mathscr{P} \to \mathscr{C} \\ Dec : \mathscr{K} \times \mathscr{C} \to \mathscr{P} \end{cases}$$

- It is said to be **exact** (resp. **approximate**) if $\forall s \in \mathscr{K}, m \in \mathscr{P}$

$$Dec_s(Enc_s(m)) = m \text{ or } Dec_s(Enc_s(m)) \approx m$$

- It is said to be **homomorphic** if $\forall s \in \mathscr{K}, m_0, m_1 \in \mathscr{P}$

$$Enc_s(m_0 \circ m_1) = Enc_s(m_0) \circ Enc_s(m_1)$$

Modulo decryption

Crypto refresher

IND-CPA: Indistinguishability under Chosen Plaintext Attack

- **IND-CPA** is a game against an adversary $\mathscr{A}$ having access to an oracle $\mathcal{O}$

  1. Game chooses $k \in \mathscr{K}$, $b \in \mathbb{B}$ and $m_0, m_1 \in \mathscr{P}$ and sends $c \leftarrow Enc_k(m_b)$ to $\mathscr{A}$
  2. $\mathscr{A}$ gets $c_i \leftarrow Enc_k(m_i)$ from $\mathcal{O}$ for messages $m_i \in \mathscr{P}$ of their choosing
  3. $\mathscr{A}$ 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