$$
\begin{aligned}
\text{Cryptosystem} &= (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}) \\
\mathcal{P} &= \text{plaintext space} \\
\mathcal{C} &= \text{ciphertext space} \\
\mathcal{K} &= \text{key space} \\
\mathcal{E} &= \{E_k \mid k \in \mathcal{K}, E_k : \mathcal{P} \to \mathcal{C})\} \\
\mathcal{D} &= \{D_k \mid k \in \mathcal{K}, D_k : \mathcal{C} \to \mathcal{P}\} \\
\forall\ e \in \mathcal{K}, \exists\ d \in \mathcal{K} \ni D_d(E_e(p)) &= p, \forall\ p \in \mathcal{P}
\end{aligned}
$$