Tutorial 3: Security against Chosen Plaintext Attacks

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. (a) Formally define (based on a security game) a notion called perfect secrecy under chosen plaintext attacks or perfect IND-CPA-security for symmetric encryption schemes (similar to perfect secrecy in the presence of an eavesdropper).
   (b) Show that there cannot exist an encryption scheme that achieves perfect IND-CPA security.

2. Let $\mathcal{E}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\mathcal{E}_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two symmetric encryption schemes over $\mathcal{M}_1, \mathcal{K}_1, \mathcal{C}_1$ and $\mathcal{M}_2, \mathcal{K}_2, \mathcal{C}_2$ respectively. You know that one of them is IND-CPA-secure and the other is not but do not know which one is actually IND-CPA-secure. Show how to build an encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ from $\mathcal{E}_1$ and $\mathcal{E}_2$ that is guaranteed to be IND-CPA-secure. You must prove that your construction is indeed IND-CPA-secure. Assume that $\mathcal{M}_1 = \mathcal{M}_2 = \{0,1\}^n$.