Exercise 1. (50 points.) Give the best IND-CPA adversary you can find against CTR-C encryption (Scheme 4.2.4 in the Bellare-Rogaway notes) when the underlying blockcipher is AES-128. Prove a lower-bound on your adversary’s advantage as a function of the total number of message-blocks in its queries, and analyze its resource-usage. For full credit your attack should be essentially best-possible (i.e., matching the upper-bound we proved in class). You may use assumptions about AES to prove your lower-bound as long as you state them precisely and (informally) justify that they are reasonable. For 25 extra points, give an unconditional attack (i.e., for which the lower-bound you prove on your adversary’s advantage holds without any unproven assumption). (Hint: Use the fact that for every key \(K\) the function \(AES_K(\cdot)\) is a permutation.)

Exercise 2. (50 points.) Alice suggests an alternative to the IND-CPA security notion for symmetric encryption, which we call IND-$\$$ security. Her definition is as follows:

Let \(SE = (K, E, D)\) be a symmetric encryption scheme. We say that \(SE\) is IND-$\$$ secure if for every “reasonable” adversary \(A\), the IND-$\$$ advantage of \(A\) defined as

\[
\text{Adv}_{SE}^{\text{ind-}\$$}(A) = 2 \cdot \Pr \left[ \text{Exp}_{SE}^{\text{ind-}\$$}(A) \text{ outputs } 1 \right] - 1
\]

is “small,” where

Experiment \(\text{Exp}_{SE}^{\text{ind-}\$$}(A)\):

\[
\begin{align*}
  b &\leftarrow_R \{0, 1\} \\
  K &\leftarrow_R K \\
  b' &\leftarrow_R A^{O}(K, b) \\
  \text{Return } (b' = b)
\end{align*}
\]

Oracle \(O(K, x, b)\):

\[
\begin{align*}
  \text{If } b = 1 \text{ then } e^* &\leftarrow_R E(K, x) \\
  \text{Else } / / b = 0 c &\leftarrow_R E(K, x) \\
  e^* &\leftarrow_R \{0, 1\}^{|c|} \\
  \text{Return } e^*
\end{align*}
\]

Intuitively, IND-$\$$ asks that the encryption of any message be indistinguishable from an independent random string of the same length as the resulting ciphertext.

Alice says that her IND-$\$$ definition is better to use than IND-CPA, because it transparently tells us that no information about the message is leaked from its encryption; after all, an independent random string clearly carries no information about the plaintext. Do you agree with her assessment? Discuss any benefits or drawbacks you see to using IND-$\$$ rather than IND-CPA.