

# CSE 794 Homework 1

Due: Thursday, January 22 by class time

1. Consider an encryption scheme  $(G, E, D)$ . Show that if the encryption algorithm  $E$  is deterministic (rather than probabilistic), then the encryption scheme cannot be multiple-ciphertext indistinguishable.
2. Show that Vernam's one-time pad is absolutely single-ciphertext indistinguishable. (Show that either of the conditions in the definition of absolute ciphertext-indistinguishability holds. It is probably easier to establish the second condition than the first one. Do not answer by just saying "Vernam's one time-pad is perfectly secret and, therefore, absolute ciphertext-indistinguishability.")
3. Show that  $A_n = \{0,1\}^n$  and  $B_n = \{s \in \{0,1\}^n : s > 2^{100}\} \cup \{1^n\}$  are polynomially indistinguishable.
4. Show that  $A_n = \{0,1\}^n$  and  $B_n = 0 \parallel \{0,1\}^{n-1}$  are polynomially distinguishable.
5. What RC4 key value will leave  $S$  unchanged during initialization? That is, after the initial permutation of  $S$ , the entries will be equal to the values from 0 through 255 in ascending order. (Hint: for what values of  $T[0..255]$ , it is always  $i = j$  in the loop of Initial Permutation so that  $S[i]$  ends up swapping with itself? Determine the value of  $T[0]$ , then  $T[1]$ ,  $T[2]$ , and so on.