Assignment 3: Due Thursday, April 24

We saw in class that in order for a symmetric encryption scheme to be CPA-secure it must be either stateful or randomized. One way to make a deterministic scheme randomized is to simply pad a portion of the plaintext with random bits. In this assignment you are to consider what security this gives for a typical symmetric block cipher.

1. Consider a basic *deterministic* symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ in which the encryption and decryption algorithms map fixed-length blocks of bits to fixed-length blocks of bits (a standard "block cipher"). Define, using the proper notation, what these functions do (make sure you specific domain, range, keyspace, etc.). Using this, create a randomized symmetric encryption scheme $\mathcal{RSE}$ that takes input blocks exactly half the length of the deterministic scheme, and pads the other half with random bits. Define the functions of this scheme as precisely as you can (give actual algorithms).

   Important note: Do this ***soon***, and if you have any question at all about whether you've done this right, come see me. If you start off wrong here, there is no way you can do the next part.

2. Come up with the best attack (an adversary A) you can against this scheme (in the ind-cpa sense). Give a precise analysis of how well your attack works, in terms of the number of oracle queries (q) and time of the adversary. You analysis so be precise enough where you end up with a formula for your adversary's advantage $\text{Adv}^{\text{ind-cpa}}_{\mathcal{RSE}}(A)$.

3. Now explore how secure this is: DES is a block cipher in which input and output blocks are 64 bits long — how many queries are necessary before the advantage is $\geq 1/2$? Do you consider this secure? AES uses blocks that are 128 bits long — how many queries are necessary before the advantage is $\geq 1/2$? Do you consider this secure?