Homework 4

1. Encrypt the King James Bible using:
   a. AES in CBC mode of operation
   b. AES in Counter Mode of Operation
   c. DES in CBC Mode of Operation
   d. DES in Counter Mode of Operation
   e. 3DES in CBC Mode of Operation
   f. 3DES in Counter Mode of Operation

   You can use a cryptographic library for implementing AES, DES and 3DES and the modes of operation. For each of the six scenarios here specified, provide your code (copy and paste into a PDF file) and the times for encryption and decryption. For which of these modes of operation can you improve the running times by exploiting parallelization?

2. Show that a CBC mode of operation is not CPA secure if the initialization vector is not random and kept constant.

3. Let F be a pseudorandom function, and G a pseudorandom generator with expansion factor $\ell(n) = n+1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. In each case, the shared key is a random $k \in \{0,1\}^n$.

   (a) To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$ and send $\langle G(k) \oplus m_1,\ G(k+1) \oplus m_2 \rangle$.

   (b) To encrypt $m \in \{0,1\}^{n+1}$, choose a random $r \leftarrow \{0,1\}^n$ and send $\langle r, G(r) \oplus m \rangle$.

   (c) To encrypt $m \in \{0,1\}^n$, send $m \oplus F_k(0^n)$.

   (d) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose $r \leftarrow \{0,1\}^n$ at random, and send $\langle r,\ m_1 \oplus F_k(r),\ m_2 \oplus F_k(r+1) \rangle$.

4. Present formulas for decryption of all the different modes of encryption we have seen. For which modes can decryption be parallelized?

Challenge (extra 25 points):

Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two encryption schemes for which it is known that at least one is CPA-secure. The problem is that you don't know which one is CPA-secure and which one may not be. Show how to construct an encryption scheme Π that is guaranteed to be CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure. Try to provide a full proof of your answer.

Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one of the parts reveals nothing about the plaintext, but knowledge of both does yield the original plaintext.