UEE4611 Assignment #6, 2020 due May 19

1. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 (Figure 7.4) obviously corrupts P_1 and P_2.
   (a) Are any blocks beyond P2 affected? (5%)
   (b) Suppose that there is a bit error in the source version of P1. Through how many ciphertext blocks is this error propagated? (5%)
   (c) How many plantext blocks are affected at the receiver (after decryption)? (5%)

2. (a) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? (5%)
   (b) How about decryption? (5%)

3. Consider DES in CFB mode with $b = 64$ and $s = 8$. Suppose the Plaintexts $P_1, P_2, \ldots, P_{80} \in \{0,1\}^8$ are encrypted to the ciphertexts $C_1, C_2, \ldots, C_{80} \in \{0,1\}^8$, respectively, and then the ciphertexts are transmitted. If a bit error occurs in the transmission of C_2, which plaintexts are affected in decryption? (10%)

4. Consider the following random number generator
$$X_{n+1} = (aX_n) \mod 2^4.$$
   (a) What is the maximum possible period of this generator? (5%)
   (b) What should be the value of a with the maximum period? (5%)
   (c) What restrictions are required on the seed in the case with maximum period? (5%)

5. RC4 has a secret internal state which is a permutation of all the possible values of the vector S and the two indices i and j.
   (a) Using a straightforward scheme to store the internal state, how many bits are used? (5%)
   (b) Suppose we think of it from the point of view of how much information is represented by the state. In that case, we need to determine how may different states there are, then take the log to base 2 to find out how many bits of information this represents. Using this approach, how many bits would be needed to represent the state? (5%)

6. Suppose you have a true random bit generator where each bit in the generated stream has the same probability of being a 0 or 1 as any other bit in the stream and that the bits are not correlated; that is the bits are generated from identical independent distribution. However, the bit stream is biased. The probability of a 1 is $0.5 + \delta$ and the probability of a 0 is $0.5 - \delta$, where $0 < \delta < 0.5$. A simple conditioning algorithm is as follows: Examine the bit stream as a sequence of nonoverlapping pairs. Then discard all 00 and 11 pairs. Replace each 01 pair with 0 and each 10 pair with 1.
   (a) What is the probability of occurrence of each pair in the original sequence? (5%)
   (b) What is the probability of occurrence of 0 and 1 in the modified sequence? (5%)
   (c) What is the expected number of input bits to produce x output bits? (5%)