Amjad Alqahtan
UTSA: wkh221
Assignment 2
Applied Cryptography

1. Yes, a PPT adversary A satisfies the requirement that the number of queries it makes to the encryption oracle is bounded by a polynomial function q(n). We bound the adversaries: $pr[A\ succeeds]\ \ <= \frac{1}{2} + \frac{q(n)}{2^n}$

   q(n) is polynomial and 2^n grows exponentially making the advantage negligible. If the adversary were allowed an exponential number of queries, the encryption insecure.

2. Since r is chosen uniformly at random $\{0, 1\}^{128}$, there are: 2^{128}, that would be the possible ciphertexts for a single plaintext message and a fixed key.
   It is not considered deterministic because different runs of encryption with the same plaintext and key will result in different ciphertexts due to the randomness in r.

3. The state st = < s, IV, i> in the stream cipher construction 3.30 requires representing n + n + log2(n) bits. Since n = 128, the total number of bits required is 128 + 128 + log2(128). So the |st|=128+128+7=263 bits.

4. Alice sends the following messages to Bob: m1 = 1000 bits, m2 = 2000 bits, and m3 = 3000 bits. Since stream ciphers do not expand message size, the ciphertext sizes remain the same as the plaintext sizes. Total ciphertext length = 1000+2000+3000 = 6000 bits.

5. We have m1 and m2 in two blocks with a block size of 256 bits. To encrypt the messages with the same key using CBC is as follows:
   a. m1 XOR IV
   b. The result will be the ciphertext c1 and the size will be the same as the block size of 256 bits
   c. m2 XOR c1 before encryption.
   d. The result will be the ciphertext c2 and the size will be the same as the block size of 256 bits
   e. Thus, the size of the ciphertext for the message M consists of m1, and m2 will be multiplied by block size, 2*256 bits.
   f. Finally, the ciphertext size for the given scenario is 512 bits.