Introduction to Cryptography

Homework 1

1. Show that property 1 holds for a cipher if and only if property 2 holds.
   - **Property 1**: For all m_1, m_2, c, it holds that Pr($Enc(m_1)=c$) = $Pr(Enc(m_2)=c)$.
   - **Property 2**: Pr(plaintext = m | ciphertext = c) = Pr (plaintext = m).

   Hint: Use Bayes law:
   Pr(plaintext=m | ciphertext=c) =
   Pr(ciphertext=c | plaintext=m) · Pr(plaintext=m) / Pr(ciphertext=c) .

2. (Error propagation in different encryption modes)
   Consider a block cipher with a 64 bit input, and three input blocks P_1,P_2,P_3. Let the input bits be numbered $p_1,\ldots,p_{192}$, where $p_1,\ldots,p_{64}$, are the bits of P_1, etc.
   The bits of the ciphertext are numbered $c_1,\ldots,c_{192}$.
   Suppose that bit c_{10} was flipped when the ciphertext was sent from A to B, but the rest of the ciphertext bits were received correctly (i.e., if the original value of bit c_{10} was 0, Bob received the value 1, and vice versa).
   For each of three encryption modes discussed in class (ECB, CBC and OFB) describe which bits of the plaintext
   a. Will surely be decrypted correctly by Bob.
   b. Will surely not be decrypted correctly by Bob.
   c. Might or might not be decrypted correctly by Bob.

   Answer the same questions when both bits c_{10} and c_{34} were flipped.

   Hint: Assume that if ciphertexts c and c' are different then any bit in the decryption of c is equal to the corresponding bit in the decryption of c' with probability ½.

3. Consider the following two variants of DES, denoted DESV and DESW, which use two keys, k and k', |k|=56 bits, |k'| = 64 bits.

   $$DESV_{k,k'}(M) = DES_k(M) \oplus k'$$
   $$DESW_{k,k'}(M) = DES_k(M \oplus k')$$

   Show that although the key length of these schemes is 120 = 56+64 bits each one of them can be broken using about 2^{56} DES encryptions/decryptions. Explain why the attacks work. Assume a known plaintext attack, i.e. that the attacker has a small number of pairs $C_i = DESW_{k,k'}(M_i)$, and $C_i = DESV_{k,k'}(M_i)$, for *randomly chosen* messages M_i.

4. Consider an implementation of 3DES of the form $C = E_{k1}(D_{k2}(E_{k1}(M)))$. Following is a meet-in-the-middle attack on this system. Assume that we want to break a specific implementation of the system, that uses the values $k_1=\alpha_1$, $k_2=\alpha_2$ for the keys k_1, k_2. Assume that the attacker has access to a "black box" implementation that computes $E\alpha_1(D\alpha_2(E\alpha_1(x)))$ for any input x, using the keys $k_1=\alpha_1$ and $k_2=\alpha_2$ used by the implementation of the encryption system that we want to break. The attack goes as follows:
    a. Generate a table that stores the value $D_{k2}(0)$ for every possible value of k_2. ("0" here refers to a string of 64 zero bits. The decryption is done using the DES algorithm.)
    b. For every possible value of k_1
        i. Compute $P = D_{k1}(0)$
        ii. Compute $Q = E\alpha_1(D\alpha_2(E\alpha_1(P)))$ (using the "black box" implementation of the encryption algorithm)
        iii. Compute $R = D_{k1}(Q)$
        iv. If R is in the table generated in step (a), mark the corresponding keys α_1, α_2 are suspects for the key used by the encryption system.
    c. Check all the suspect keys marked by step b(iv).

    Explain why this attack works.
    Estimate the overhead of the attack.
    Explain why this attack is less severe than the meet-in-the-middle attack discussed in class.
    Explain why we can replace the value "0" used in steps (a) and b(i) by any arbitrary value, as long was use the same value in both steps.

    Hint: Note that the messages P generated in step b(i) are the messages for which the first step of 3DES, namely E_{k1}, results in a intermediate value equal to 0.