Introduction to Cryptography

Homework 1

Due by November 20, 2005 (before class).

1. For any cipher, the following two properties are equivalent.
   - **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).

   Prove *one* of the following two statements.
   - If Property 1 is true then so is Property 2.
   - If Property 2 is true then so is Property 1.

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

2. (Shannon's theorem)
   Consider an encryption scheme where the size of the plaintext space *(P)* is equal to the size of the ciphertext space *(C)*, and is also equal to the size of the key space *(K)*. (Namely $|P|=|C|=|K|$.) Then the encryption scheme provides perfect secrecy *if and only if* the following two conditions hold:
   - Every key is chosen with equal probability ($1/|K|$).
   - For every message *m* in *P* and every possible ciphertext *c* in *C*, there exists a single key *k* in *K*, such that $E_k(m)=c$.

   Prove *one* of the two directions of the theorem (namely, either the "if" direction or the "only if" direction.).

3. (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,…,p_{192}, where p_1,…,p_{64}, are the bits of P_1, etc.
   The bits of the ciphertext are numbered c_1,…,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.