T-79.4501 Cryptography and Data Security
2006 / Homework
Mon 6.2 and Wed 8.2

1. DESX was proposed by R.Rivest to protect DES against exhaustive key search. DESX uses one 64-bit secret key W to perform pre- and postwhitening of data and a 56-bit DES key K, and operates as follows:

   $$C = W \oplus E_K(P \oplus W)$$

   Originally two different keys were used for pre- and postwhitening, but Kilian and Rogaway showed (Crypto '96) that the same key can be used for both. Show that a similar construction

   $$C = W \oplus E_K(P)$$

   without prewhitening is insecure, and can be broken using an attack of complexity 2^{56}.

2. Consider an LFSR with feedback polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$.
   (a) What are the cycles (periods) of the sequences generated by this LFSR?
   (b) Compute the values for the autocorrelation function for each cycle.

3. Consider a threshold generator (Lecture 4) with three LFSRs defined by the connection polynomials and initial states:

   $$\begin{aligned} f_1(x) &= x^2 + x + 1, \text{ initial state } \texttt{01} \\ f_2(x) &= x^3 + x + 1, \text{ initial state } \texttt{001} \\ f_3(x) &= x^3 + x^2 + 1, \text{ initial state } \texttt{001} \end{aligned}$$

   Compute the first 30 bits of the output sequence of the threshold generator.
   (a) Is the output sequence balanced, that is, has it about equally many zeroes and ones?
   (b) Compare the bits of the output sequence and the corresponding bits of the sequence generated by the third LFSR. For how many bits they are equal?

4. We consider a polynomial MAC with 4-bit coefficients in the Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. Given an one time pad = 0110, and a point X = 0011, evaluate the polynomial MAC for the message $P = (P_0, P_1, P_2)$ = 101010111100.

5. Consider the following two ways of specifying an initialisation of a 64-bit input field for counter mode of a 64-bit block cipher:
   (a) The 64-bit input block is divided into two 32-bit fields, IV and CTR. For each new key we set IV = 0. For each new message IV is incremented by 1 and CTR is set equal to 0.
   (b) For each new message a 64-bit random number R is generated and the 64-bit counter is initialised with R.

   Estimate in both cases how many initialisations (new messages) can take place before the risk of having two equal initial input fields is too big.

6. (a) Show that the bitwise operation of the function $F_t(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ used in SHA-1 is exactly the same as the operation of the threshold function (also called as majority function) t used in the threshold key stream generator (see Lecture 4).
   (b) Show that the threshold function can also be expressed as $t(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ where the addition and multiplication is computed modulo 2. In particular this means that the function F_t has another equivalent presentation as $F_t(B, C, D) = (B \wedge C) \oplus (B \wedge D) \oplus (C \wedge D)$.