T-79.159 Cryptography and Data Security
2005 / Homework
Tue 5.4 and Fri 8.4

1. (a) Prove 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) 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 meands that the SHA-1 function has another equivalent presentation as $F_t(B, C, D) = (B \wedge C) \oplus (B \wedge D) \oplus (C \wedge D)$.

2. 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

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

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

3. Assume that an HMAC are using SHA-1 as the underlying hash function. What changes are required in the implementation if SHA-1 is replaced by SHA-256?

4. For SHA-1, show the values of W_{16},W_{17}, W_{18} and W_{19}.

5. Using RFC 3610 describe how the input data is formatted in the CCM mode of operation. What is the role of the nonce? Give an example, how the nonce can be constructed in practise (see NIST SP800-38C, for example).