T-79.503 Fundamentals of Cryptology
Homework 8
November 5, 2002

1. The standard hash-function SHA-1 makes use of two non-linear combination functions. The first of them, G, was examined at the lecture. The second one is denoted by T and it is defined as follows. Let X_0, X_1, X_2 be three 32-bit words. Then

$$T(X_0, X_1, X_2) \quad = \quad (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$$

   Let t denote the one-bit component of T.

   a) Create the value table for t. (This function is also known as the "threshold-function". It takes the value "1" exactly when at least two of the input-variables take the value "1".)

   b) Compute the difference distribution table $N_D(a', b')$ of t. (Note that t can be considered as an S-box with three-bit input and one-bit output.)

   c) A *linear structure* of a Boolean function f of three variables is defined as a vector $w = (w_1, w_2, w_3) \neq (0, 0, 0)$ such that $f(x \oplus w) \oplus f(x)$ is constant. Show that t has exactly one linear structure.

2. (Stinson 4.11) A message authentication code can be produced by using a block cipher in CFB mode instead of CBC mode. Given a sequence of plaintext blocks, $x_1, x_2, \ldots, x_n$, suppose we define the initialization vector IV to be x_1. Then encrypt the sequence $x_2, \ldots, x_n$ using key K in CFB mode, obtaining the ciphertext sequence $y_1, \ldots, y_{n-1}$ (note that there are only $n-1$ ciphertext blocks). Finally, define the MAC to be $e_K(y_{n-1})$ Prove that this MAC is identical to the MAC produced in Section 4.4.2 using CBC mode.

3. Assume that a sequence of plaintext blocks of length 128 bits have been encrypted using the AES block cipher in CBC mode.

   a) How many blocks need to be encrypted so that the probability of finding two equal ciphertext blocks becomes larger than 0.5?

   b) If two equal ciphertext blocks are detected, what can be said about the corresponding plaintext blocks?

4. (Stinson 5.10) Suppose that $n = pq$ where p and q are distinct odd primes and $ab \equiv 1(\bmod (p-1)(q-1))$. The RSA encryption operation is $e(x) = x^b \bmod n$ and the decryption operation is $d(y) = y^a \bmod n$. We proved that $d(e(x)) = x$ if $x \in \mathbb{Z}_n^*$. Prove that the same statement is true for any $x \in \mathbb{Z}_n$.

5. Bob is using RSA cryptosystem and his modulus is $n = pq = 29 \times 2003 = 58087$. Bob chooses an odd integer for his public encryption exponent b. Prove that if the plaintext is 2002 then the ciphertext is equal to 2002.