T-79.503 Fundamentals of Cryptology
Homework 8
November 11, 2004

1. (Stinson 3.9) Suppose that $\mathbf{X}_1, \mathbf{X}_2$ and $\mathbf{X}_3$ are independent random variables defined on the set $\{0, 1\}$. Let ϵ_i denote the bias of $\mathbf{X}_i$ for $i = 1, 2, 3$. Further, let us denote by ϵ_{ij} the bias of the random variable $\mathbf{X}_i \oplus \mathbf{X}_j$, for $i \neq j$. Prove that if $\mathbf{X}_1 \oplus \mathbf{X}_2$ and $\mathbf{X}_2 \oplus \mathbf{X}_3$ are independent then $\epsilon_1 = 0$, or $\epsilon_3 = 0$, or $\epsilon_2 = \pm\frac{1}{2}$.

2. 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?

3. Let e_K be the encryption transformation of a block cipher with 64-bit key K and 64-bit block length. The key size of the block cipher is doubled as follows. Given two 64-bit keys K_1 and K_2 and a 64-bit plaintext x the ciphertext y is computed as

$$y = e_{K_2}(x \oplus K_1).$$

   Assume that an attacker has two known plaintext-ciphertext pairs x_1, y_1 and x_2, y_2 encrypted in this manner with a 128-bit key (K_1, K_2). Show that then the attacker can find the used 128-bit key with a large probability, by doing exhaustive search over a 64-bit partial key.

4. The standard hash-function SHA-1 makes use of two non-linear combination functions. 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. The Boolean function t is also called as "threshold function" since it takes value 1 exactly if at least two of the inputs are equal to 1.

   a) Create the value table for t.

   b) Find the algebraic normal form of t.

   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.

5. (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.