T-79.5501 Cryptology
Homework 6
November 3 & 4, 2005

1. Consider the example linear attack in Stinson, section 3.3.3. In S_2^2 replace the random variable $\mathbf{T}_2$ by $\mathbf{U}_6^2 \oplus \mathbf{V}_8^2$. Then in the third round the random variable $\mathbf{T_3}$ is not needed. What is the final random variable corresponding to formula (3.3) (page 87) and what is its bias?

2. Consider the 4-bit to 4-bit function f determined by the third row of S-box S_1 of DES:

   `4 1 E 8 D 6 2 B F C 9 7 3 A 5 0`

   Let us set $a = 4 =$ `0100`. Which values the difference $f(x \oplus a) \oplus f(x)$ takes as x varies through all sixteen values $x = (x_1, x_2, x_3, x_4)$?

3. Consider the finite field $GF(2^3) = \mathbb{Z}_2[x]/(f(x))$ with polynomial $f(x) = x^3 + x + 1$ (see Stinson 6.4).

   (a) Compute the look-up table for the inversion function $f : z \mapsto z^{-1}$ in $GF(2^3)$, where we set $f(0) = 0$.

   (b) Compute the algebraic normal form of the Boolean function defined by the least significant bit of the inversion function.

4. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$ and let $f : \mathbb{F} \to \mathbb{F}$ be a function defined as

$$\begin{aligned} f(z) &= z^{-1}, \text{ for } z \neq 0, \\ f(0) &= 0. \end{aligned}$$

   Let a Feistel cipher be defined as follows

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1} \oplus K_i), \end{aligned}$$

   where $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$ and the round keys are defined as $K_i = K^i$, for $i = 1, 2, 3$, where $K \in \mathbb{F}$ is the key. Assume that one known plaintext-ciphertext pair is given as follows: $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ and $R_3 = 100$. Attempt to find the key K.

5. Consider the “threshold function” t: $(\mathbb{Z}_2)^3 \to \mathbb{Z}_2$, $t(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$, where the bit operations are the usual modulo 2 addition and multiplication. (See: Backgound paper on Boolean functions, Example 6.)

   (a) Compute the values of the difference distribution table $N_D(a', b')$ of the function t, for $a' = 010$ and $a' = 111$ and all $b' \in \mathbb{Z}_2$.

   (b) Show that t preserves complementation, that is, if each input bit is complemented then the output is complemented.

6. Consider the Galois field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))$ where $f(x)$ is a polynomial of degree n. We define a function $h : z \mapsto z^3$, for $z \in \mathbb{F}$. This function defines a n-bit to n-bit S-box.

   (a) Prove that this S-box is almost perfect nonlinear, that is, all entries in the difference distribution table $N_D(a', b')$ are either 0 or 2, for all $a' \neq 0$ and $n \geq 3$.

   (b) For which values of n this S-box is bijective?