T-79.503 Fundamentals of Cryptology
Homework 7
November 4, 2004

1. Consider the finite field $GF(2^3)$ with polynomial $x^3 + x + 1$ (see Stinson 6.4).
   (a) Create the look-up table for the inversion function $z \mapsto z^{-1}$ in $GF(2^3)$.
   (b) Compute the algebraic normal form of the Boolean function defined by the least significant bit of the inversion function.
2. Compute the linear approximation table (values $N_L(a, b)$) for the substitution transformation defined by the inversion mapping (see exercise 1(a)).
3. Consider Galois field $\mathbb{F} = GF(2^8)$ with polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. The elements of $\mathbb{F}$ are given as octets using hexadecimal notation. Suppose that two polynomials $c(x)$ and $d(x)$ with coefficients in $\mathbb{F}$ are given as follows:

$$\begin{aligned} c(x) &= '03'x^3 +' 01'x^2 +' 01'x +' 02' \\ d(x) &= '0B'x^3 +' 0D'x^2 +' 09'x +' 0E' \end{aligned}$$

   Show that $c(x)d(x) =' 01' (\text{mod } x^4 +' 01')$. The polynomial $c(x)$ defines the MixColumn transformation in Rijndael and $d(x)$ defines its inverse transformation.
4. Consider the Galois field $GF(2^n) = \mathbb{Z}_2[x]/f(x)$ where $f(x)$ is a polynomial of degree n. We define a mapping in it as $z \mapsto z^3$, for $z \in GF(2^n)$. This mapping defines a n-bit to n-bit S-box in a natural manner.
   (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 $n \geq 3$.
   (b) For which values of n this S-box is bijective?
5. 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 in formula (3.3) (page 87) and what is its bias?