T-79.503 Basics of Cryptology
Homework 7
October 29, 2003

1. 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 $c(x)d(x) = 01'(\bmod\ x^4 +' 01')$. The polynomial $c(x)$ defines the MixColumn transformation in Rijndael and $d(x)$ defines its inverse transformation.

2. Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables defined on the set $\{0, 1\}$. Let ϵ_i denote the bias of $\mathbf{X}_i$, $\epsilon_i = Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, for $i = 1, 2$. Prove that if the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent, then $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

3. Consider the finite field $GF(2^3)$ with polynomial x^3+x+1 and inversion function $z \mapsto z^{-1}$ in $GF(2^3)$ (see Stinson 6.4 and last week's homework problem 5). Compute the linear approximation table (values $N_L(a', b')$)for this substitution transformation.

4. 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?

5. Consider the Galois field $GF(2^n)$. Prove that the mapping $z \mapsto z^3$ is *almost perfect nonlinear*, that is, the values $N_D(a', b')$ in the difference distribution table of the S-box defined by this mapping are equal to 0 or 2.