T-79.5501 Cryptology
Homework 7
March 13, 2007

1. 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 Handout 3, 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 $b' \in \{0, 1\}$.
   (b) Show that t preserves complementation, that is, if each input bit is complemented then the output is complemented.

2. Consider the Galois field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))=$ GF(2^n), 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?

3. Determine the two least significant decimal digits of the integer 2007^{2007}.

4. (Stinson 5.9) Suppose that $p = 2q + 1$, where p and q are odd primes. Suppose further that $\alpha \in \mathbb{Z}_p^*$, $\alpha \neq \pm 1 (\mathrm{mod} p)$. Prove that α is a primitive element modulo p if and only if $\alpha^q \equiv -1 \, (\mathrm{mod} p)$.

5. Find the smallest primitive element in $\mathbb{Z}_{23}^*$. (Hint: use the result of problem 4.) What are the orders of elements 2 and 4? Give 2 and 4 as powers of the smallest primitive element.

6. Bob is using RSA cryptosystem and his modulus is $n = pq = 59 \times 251 = 14809$. Bob chooses an odd integer for his public encryption exponent b. Show that if the plaintext is 2007 then the ciphertext is equal to 2007.