Wrocław University of Technology, WPPT 18.11.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 5

1. Evaluate the speed of avalanche effect for AES. Consider different versions of the block length (look for an exact specification of AES in the Web).

2. (a) Find an irreducible polynomial of degree 8 over $GF(2)$.
   (b) Construct a finite field of cardinality 2^8.
   (c) In this field multiply the elements $x^7 + x^5 + x^4 + 1$ by $x^6 + x^3 + x^2 + x + 1$.

3. Find and prove the recursive formula for finding x, y such that

$$x \cdot a + y \cdot b = GCD(a, b)$$

   using extended Euclidean algorithm.

4. Is it possible to use the binary GCD algorithm for computing inverses modulo p for a prime number p? If no, then provide a suitable extension. In any case estimate the resulting runtime.

5. Find a reasonable choice of the parameters for finding discrete logarithm with baby-step giant-step algorithms on a typical PC.

6. let us consider the Floyd method applied for Pollard rho algorithm for finding discrete logarithms. Assume that we would like to save time and instead of computing x_i and x_{2i} for $i = 1, 2, \ldots$, we postpone a little bit and start from some j: we compute x_{j+i} and x_{j+2i} for $i = 1, 2 \ldots$.
   How to choose j?

/-/ Mirosław Kutyłowski and Filip Zagórski