4. Problem Set

Secure Channels

(Winter Term 2014/2015)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Jakob Wenzel (jakob.wenzel@uni-weimar.de)
URL: http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/

Date: 02.12.2014 (1:30 pm) **Room:** SR013, B11

Goal of this Problem Set: First, you should remember/refresh and test your knowledge about Galois fields (finite fields). Second, you will understand some essential design choices for certain MAC constructions.

- Submit your solutions until **1st of December 2014, 12:00 am** via E-Mail or feed my postbox in Room 112. Clearly, at least the .py file should be sent via E-Mail.
- The python source code file should have the format `<matriculation number>.py`. One matriculation number per group if sufficient. Write the name and the matriculation number of all group members in the header of the python file.

Task 1 (8 Credits) Repetition: Galois Field (Finite Field)

a) Test each of the following polynomials f_i regarding to whether it is an irreducible polynomial. Assume that the coefficients are from the stated fields F.

1) $f_1(x) := x^2 + 1$ with $F = \mathbb{Z}_2$
2) $f_2(x) := x^2 + x + 1$ with $F = \mathbb{Z}_2$
3) $f_3(x) := x^4 + 2x^2 + x$ with $F = \mathbb{Z}_3$

b) Consider the finite field $F[X]_{p(x)}$ with the reduction polynomial $p(x) = x^3 + x + 1$. Thus, we consider the finite field $\mathbb{Z}_2[X]_{x^3+x+1}$. Postulate the addition and multiplication table for each element from this finite field.

c) Show that $p(x) = x^2 + x + 1$ is the only irreducible polynomial of order 2 with coefficients from $\mathbb{Z}_2$.

d) Let F be a finite field. Show that a polynomial $p(x)$ from $F[X]$ of order 2 or 3 is an irreducible polynomial if and only if $p(a) \neq 0$ for all values of $a \in F$.

Task 2 (2 Credits) Encrypted CBC-MAC
Show that the Encrypted CBC-MAC (as defined on Slide 70) is vulnerable in the UF-CMA scenario if $K_1 = K_2$ by describing an efficient adversary.

Task 3 (2 Credits) CMAC'
Let CMAC be defined as on Slide 74. Consider a variant of CMAC, called CMAC', where $L = 0$. Show that CMAC' is vulnerable in the UF-CMA scenario by describing an efficient adversary.

Task 4 (4 Credits) PMAC
Let PMAC be defined as on Slide 76.

a) Describe an adversary which is allowed to ask $q \leq 2^{b/2}$ queries to a PMAC oracle $\mathcal{O}$, where b describes the block length of the underlying block cipher.

b) Let PMAC' be a variant of PMAC where $L = 0$. Show that PMAC' is vulnerable in the UF-CMA scenario exploiting this fact by describing an efficient adversary.

Task 5 (8 Credits) Programming Task – Galois Field $GF(2^8)$
Write a python library which implements the Galois field arithmetic for $GF(2^8)$. Your library should contain at least the following functionality:

- initialization of a field defined by an irreducible polynomial
- addition/multiplication of polynomials modulo an irreducible polynomial
- subtraction/division of polynomials modulo an irreducible polynomial
- computation of the multiplicative inverse (required for division)

Note that in fields, the division is represented by the multiplication with the multiplicative inverse, e.g., $a/b = a \cdot b^{-1}$*, where* b^{-1} *denotes the multiplicative inverse of* b *in the certain field.*