# Exercise 3

Module 1 - Introduction to Cryptography and Data Security

Knut Lucas Andersen
Master Applied Information Security
isits AG International School of IT Security

May 16, 2017

# Contents

## 1 Addition in $\mathbf{GF(2^8)}$

**a)** $\mathbf{A(x) = x^7 + x^5 + x^3 + x^2 + 1, B(x) = x^4 + x^3 + 1}$

**b)** $\mathbf{A(x) = x^5 +} {}^{x3} \mathbf{+ x^2, B(x) = x^6 + x^4 + x^3 + 1}$

**c)** $\mathbf{A(x) = x^6 + x^5 + x^3 + x + 1, B(x) = x^7 + x^6 + x^4 + x^2 + 1}$

**d) Which effect has the reduction polynome in general on the result of an addition?**

## 2 Multiplication in $\mathbf{GF(5^4)}$

Consider the finite field $\mathrm{F}(5^4)$ with the irreducible reduction polynome $\mathrm{P(x)} = \mathrm{x}^4 + \mathrm{x}^2 + 2\mathrm{x} + 2$.

a) Compute the addition table for this field

b) Compute the multiplication table for this field.

c) Compute $x^4$ mod P(x), $x^5$ mod P(x) and $x^6$ mod P(x).

d) Calculate A(x) × B(x) mod P(x) for A(x) = $x^4 + x^1 + 2$, B(x) = $2x^3 + 2x^2 + 1$

## 3 Multiplication in GF($2^8$)

a) Compute A(x) × B(x) mod P(x) for the following values and give the result in HEX

b) With which operation is it possible to realise both these multiplications $B_1(x) = x$, $B_2(x) = x+1$ efficiently

## 4 Avalanche effect in AES

a) Calculate the respective Output to the Input W after the first round of AES! use the round-keys $K_0, \dots, K_1$!

b) Compute all the output bytes for the case that all the input bytes are zero (solution only in HEX)

c) How many outputbytes have changed now? (We consider just one round of AES)

## 5 Keygeneration in AES

a) Given is a main key K, consisting of zeros. Find the sub-key $K_1$ after the first round of key-generation.

b) Given is the main key K = (0x00000008; 0x00000004; 0x00000002; 0x00000001). Find the sub-key $K_1$ after the first round of key-generation.

## 6 Solution template for Avalanche effect in AES

a) After conversion of the Input in matrix-form

b) After conversion of the Input in matrix-form