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 30, 2017

Contents

1 Addition in GF(2^8)

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

Since addition uses XOR, I have "padded" the equation with zero's to better display the difference (and equality) between A(x) and B(x). For this, the LaTeX *frac{num}{den}* was used.

$$A(x) = x^7 + x^5 + x^3 + x^2 + 1,$$
$$B(x) = x^4 + x^3 + 1$$

Comparison listing:

$$+\frac{A(x)}{B(x)} \Rightarrow +\frac{x^7 + 0 + x^5 + 0 + x^3 + x^2 + 0 + 1}{0 + 0 + 0 + x^4 + x^3 + 0 + 0 + 1} \tag{1}$$

Modulus 2 cancels out those that are equal:

$$A(x) + B(x) \Rightarrow x^7 + x^5 + x^4 + (1+1)x^3 + x^2 + (1+1)$$
$$A(x) + B(x) \Rightarrow x^7 + x^5 + x^4 + 0x^3 + x^2 + 0$$
$$\underline{\underline{A(x) + B(x) = x^7 + x^5 + x^4 + x^2}}$$

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

$$A(x) = x^5 + x^3 + x^2,$$
$$B(x) = x^6 + x^4 + x^3 + 1$$

Comparison listing:

$$+\frac{A(x)}{B(x)} \Rightarrow +\frac{0 + x^5 + 0 + x^3 + x^2 + 0 + 0}{x^6 + 0 + x^4 + x^3 + 0 + 0 + 1} \tag{2}$$

Modulus 2 cancels out those that are equal:

$$A(x) + B(x) \Rightarrow x^6 + x^5 + x^4 + (1+1)x^3 + x^2 + 1$$
$$A(x) + B(x) \Rightarrow x^6 + x^5 + x^4 + 0x^3 + x^2 + 1$$
$$\underline{\underline{A(x) + B(x) = x^6 + x^5 + x^4 + x^2 + 1}}$$

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

$$\begin{aligned} A(x) &= x^6 + x^5 + x^3 + x + 1, \\ B(x) &= x^7 + x^6 + x^4 + x^2 + 1 \\ &\textit{Comparison listing:} \\ +\frac{A(x)}{B(x)} &\Rightarrow +\frac{0 + x^6 + x^5 + 0 + x^3 + 0 + x + 1}{x^7 + x^6 + 0 + x^4 + 0 + x^2 + 0 + 1} \end{aligned} \tag{3}$$

Modulus 2 cancels out those that are equal:

$$A(x) + B(x) \Rightarrow x^7 + (1+1)x^6 + x^5 + x^4 + x^3 + x^2 + x + (1+1)$$
$$A(x) + B(x) \Rightarrow x^7 + 0x^6 + x^5 + x^4 + x^3 + x^2 + x + 0$$
$$\underline{\underline{A(x) + B(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x}}$$

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

The reduction polynome in general has a XOR effect both for addition and substitution. This means you can just use the XOR to find the result, because each number is its additive inverse.

2 Multiplication in GF(5^4)

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

a) Compute the addition table for this field

b) Compute the multiplication table for this field.

c) Compute $\mathbf{x^4}$ mod P(x), $\mathbf{x^5}$ mod P(x) and $\mathbf{x^6}$ mod P(x).

$$\begin{aligned} &x^4 mod P(x), x^5 mod P(x) \\ &x^6 mod P(x) \end{aligned} \tag{4}$$

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

$$\begin{aligned} &A(x) \times B(x) \ mod \ P(x); \\ &A(x) = x^4 + x^1 + 2, \\ &B(x) = 2x^3 + 2x^2 + 1 \end{aligned} \tag{5}$$

3 Multiplication in GF(2^8)

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

a).1 $\mathbf{A(x) = x^7 + x^4 + x^{x3} + x + 1}$, $\mathbf{B(x) = x}$

$$\begin{aligned} A(x) &= x^7 + x^4 + x^{x3} + x + 1, \\ B(x) &= x \end{aligned} \tag{6}$$

a).2 $\mathbf{x^6 + x^3 + x + 1}$, $\mathbf{B(x) = x + 1}$

$$\begin{aligned} A(x) &= x^6 + x^3 + x + 1, \\ B(x) &= x + 1 \end{aligned} \tag{7}$$

a).3 $\mathbf{x^7 + x^6 + x^5}$, $\mathbf{B(x) = x^3 + x}$

$$\begin{aligned} A(x) &= x^7 + x^6 + x^5, \\ B(x) &= x^3 + x \end{aligned} \tag{8}$$

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!

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