DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Exercise: **Finite Fields**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-19

1. Fill in the missing values ($GF(2^m)$)

Polynomial	Binary	Decimal
$x^7 + x^6 + x^4 + x + 1$		
	11001001	
		133
$x^4 + x^2 + x$		
	00011001	
		10

Solution

Polynomial	Binary	Decimal
$x^7 + x^6 + x^4 + x + 1$	11010011	211
$x^7 + x^6 + x^3 + 1$	11001001	201
$x^7 + x^2 + 1$	10000101	133
$x^4 + x^2 + x$	00010110	22
$x^4 + x^3 + 1$	00011001	25
$x^3 + x$	00001010	10

2. In $GF(2^5)$ with irreducible polynom $p(x) = x5 + x2 + 1$

- Calculate: $(x^3 + x^2 + x + 1) - (x + 1)$

Solution

$x^3 + x^2$

- Calculate: $(x^4 + x) \times (x^3 + x^2)$

> **Solution**
>
> $f(x) = (x^4 + x) \cdot (x^3 + x^2)\ mod\ p(x) = x^7 + x^6 + x^4 + x^3\ mod\ p(x) = x^2 + x$

- Calculate: $(x^3) \times (x^2 + x^1 + 1)$

> **Solution**
>
> $x^4 + x^3 + x^2 + 1$

- Calculate: $(x^4 + x)/(x^3 + x^2)$ given $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

  Recall: Division can be defined in terms of multiplication: if $a, b \in F$ then $a/b = a \times (b^{-1})$, where b^{-1} is called the inverse of b.

> **Solution:**
>
> $x^4 + 1$

- Verify: $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

> **Solution**
>
> Result is 1 (rest).

3. In $GF(2^8)$

   Let's assume that 7 and 3 are representatives of the bit patterns of the coefficients of the polynomial.

   - Calculate: $7d - 3d$
   - Calculate: $7d + 3d$

> **Solution**
>
> ```
> 7 = 0000 0111
> 3 = 0000 0011
> xor =>.. 0100
> ```
>
> Solution in both cases: 4 (i.e., addition and subtraction is the same; every value is its additive inverse.)

- Calculate: $(0x03 \times 0x46)$

Solution

$03 \times 46 = 46 \oplus (02 \times 46)$

$= 0100\,0110_b \oplus 1000\,1100_b = 1100\,1010_b = 202_d = 0xCA$