DHBW
Duale Hochschule
Baden-Württemberg
CAS
Center for Advanced Studies

IT-Security Cryptography and Secure Communications

Excercise: **Finite Fields**
Lecturer: *Prof. Dr. Michael Eichberg*
Version: 2023-10-12

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

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

   - Calculate: $(x^3 + x^2 + x + 1) - (x + 1)$
   - Calculate: $(x^4 + x) \times (x^3 + x^2)$
   - Calculate: $(x^3) \times (x^2 + x^1 + 1)$
   - 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.
   - Verify: $(x^3 + x^2)^{-1} = (x^2 + x + 1)$

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: $7d + 3d$
   - Calculate: $(0x03 \times 0x46)$ (use both approaches)