

Homework 2
2022-2023 3rd Trimester
Due on Saturday May 6, 2023, 11:59 p.m. via Blackboard.

If you do not have the textbook, use the following link to download it

<https://emadalsuwat.github.io/cryptography/textbook1.pdf>

Do textbook problems:

- Problem 4.6 (Page 142)
- Problem 4.7 (Page 142)
- Problem 4.13 (Page 143)
- Problem 4.15 (Page 143)
- Problem 4.19 (Page 144)
- Determine the multiplicative inverse of $x^3 + 1$ in $GF(2^4)$
- Determine the multiplicative inverse of $x^3 + x + 1$ in $GF(2^4)$
- Addition in $GF(2^4)$: Compute $A(x) + B(x) \bmod P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of the reduction polynomial on the computation?

1. $A(x) = x^2 + 1, B(x) = x^3 + x^2 + 1$

2. $A(x) = x^2 + 1, B(x) = x + 1$

- Multiplication in $GF(2^4)$: Compute $A(x) \cdot B(x) \bmod P(x)$ in $GF(2^4)$ using the irreducible polynomial $P(x) = x^4 + x + 1$. What is the influence of the choice of the reduction polynomial on the computation?

1. $A(x) = x^2 + 1, B(x) = x^3 + x^2 + 1$

2. $A(x) = x^2 + 1, B(x) = x + 1$

- Problem 5.4 (Page 179)