Assignment 8

Konstantinos Filippou
ics23044

Exercise 1

Construct the 8×8 multiplication table for the extension field

$$\mathbb{F}(2^3)$$

with irreducible polynomial

$$P(x) = x^3 + x^2 + 1.$$

Solution

Let:

$$\mathbb{F}(2^3) = \mathbb{F}_2[x]/(x^3 + x^2 + 1).$$

Elements:

$$\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}.$$

The multiplication table is computed modulo $P(x)$. (Generated programmatically in Sage.)

```
K.<a> = GF(2)[]
F.<x> = GF(2^3, modulus=x^3 + x^2 + 1)
elements = list(F)
mult_table = [[a*b for b in elements] for a in elements]

for row in mult_table:
    print(row)
```

```
[0, 0, 0, 0, 0, 0, 0, 0]
[0, x^2, x^2 + 1, x^2 + x + 1, x + 1, x^2 + x, 1, x]
[0, x^2 + 1, x^2 + x + 1, x + 1, x^2 + x, 1, x, x^2]
[0, x^2 + x + 1, x + 1, x^2 + x, 1, x, x^2, x^2 + 1]
[0, x + 1, x^2 + x, 1, x, x^2, x^2 + 1, x^2 + x + 1]
[0, x^2 + x, 1, x, x^2, x^2 + 1, x^2 + x + 1, x + 1]
[0, 1, x, x^2, x^2 + 1, x^2 + x + 1, x + 1, x^2 + x]
[0, x, x^2, x^2 + 1, x^2 + x + 1, x + 1, x^2 + x, 1]
```

Figure 1:

Exercise 2

Compute

$$C(x) = (A(x) + B(x)) \bmod P(x)$$

in $\mathbb{F}(2^4)$ with irreducible polynomial

$$P(x) = x^4 + x^3 + 1.$$

Case 1

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

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

Since addition in $\mathbb{F}_2$ is XOR:

$$C(x) = x^3.$$

Case 2

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

$$C(x) = (x^2 + 1) + (x + 1) = x^2 + x.$$

Remark

The choice of irreducible polynomial does not affect addition, since addition is coefficient-wise modulo 2.

Exercise 3

Case 1

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

$$C(x) = A(x) \cdot B(x) = (x^2 + 1)(x^3 + x^2 + 1).$$

$$= x^5 + x^4 + x^3 + 1.$$

Using:

$$x^4 \equiv x^3 + 1 \pmod{P(x)},$$

we reduce:

$$C(x) = x^3 + x + 1.$$

Case 2

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

$$C(x) = (x^2 + 1)(x + 1) = x^3 + x^2 + x + 1.$$

Since degree < 4, no reduction is needed.

Remark

Reduction is required only when the degree of the result is greater than or equal to the degree of $P(x)$.

Exercise 4

Compute inverses in $\mathbb{F}(2^8)$ with irreducible polynomial:

$$x^8 + x^4 + x^3 + x + 1.$$

Results:

$$\texttt{0x91} \to x^7 + x^4 + 1, \quad \text{inverse} = x^6 + x^5 + x^3 + x.$$

$$\texttt{0xC3} \to x^7 + x^6 + x + 1, \quad \text{inverse} = x^7 + x^5 + x + 1.$$

$$\texttt{0xDA} \to x^7 + x^6 + x^4 + x^3 + x, \quad \text{inverse} = x^7 + x^6 + x^2.$$

$$\texttt{0x6B} \to x^6 + x^5 + x^3 + x + 1, \quad \text{inverse} = x^7 + x^6 + x^4 + x^3 + x^2 + x + 1.$$

$$\texttt{0x22} \to x^5 + x, \quad \text{inverse} = x^6 + x^4 + x^3 + x.$$

We verify program:

```
K.<a> = GF(2)[]
F.<x> = GF(2^8, modulus=a^8 + a^4 + a^3 + a + 1)

print("Irreducible polynomial:", F.modulus())
print()

hex_vals = [0x91, 0xC3, 0xDA, 0x6B, 0x22]

def int_to_GF256(n):
    return sum(((n >> i) & 1) * x^i for i in range(8))

elements = [int_to_GF256(v) for v in hex_vals]

inverses = [e^-1 for e in elements]

for h, e, inv in zip(hex_vals, elements, inverses):
    print("Element:", hex(h))
    print("As polynomial:", e)
    print("Inverse:", inv)
    print("Check:", e * inv)
    print()
```

Figure 2:

```
Irreducible polynomial: x^8 + x^4 + x^3 + x + 1

Element: 0x91
As polynomial: x^7 + x^4 + 1
Inverse: x^6 + x^5 + x^3 + x
Check: 1

Element: 0xc3
As polynomial: x^7 + x^6 + x + 1
Inverse: x^7 + x^5 + x + 1
Check: 1

Element: 0xda
As polynomial: x^7 + x^6 + x^4 + x^3 + x
Inverse: x^7 + x^6 + x^2
Check: 1

Element: 0x6b
As polynomial: x^6 + x^5 + x^3 + x + 1
Inverse: x^7 + x^6 + x^4 + x^3 + x^2 + x + 1
Check: 1

Element: 0x22
As polynomial: x^5 + x
Inverse: x^6 + x^4 + x^3 + x
Check: 1
```

Figure 3:

Exercise 5

AES first round computation.

Given

State: 128 bits = 16 bytes, all equal to `0x01`.

Round key: 128 bits = 16 bytes, all equal to `0x01`.

AddRoundKey

$$0x01 \oplus 0x01 = 0x00.$$

Thus state becomes all zeros.

SubBytes

S-box substitution:

$$S(0x00) = 0x63.$$

Thus all bytes become `0x63`.

ShiftRows

Since all bytes are identical, the state remains unchanged.

MixColumns

Each column is multiplied by the AES matrix:

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}.$$

Since all entries are `0x63`:

$$(2 \cdot 0x63) \oplus (3 \cdot 0x63) \oplus (1 \cdot 0x63) \oplus (1 \cdot 0x63) = 0x63.$$

Thus state remains all `0x63`.

Add Round Key

$$0x63 \oplus 0x01 = 0x62.$$

Final state:

62	62	62	62
62	62	62	62
62	62	62	62
62	62	62	62