Université Libre de Bruxelles
Faculté des Sciences

2023-2024

INFO-F-405: Introduction to cryptography

Introduction to the finite field GF(2^8)

The goal of this session is to recall the basic properties of the field GF(256) used in AES .

Finite fields are algebraic structures in which one can apply the basic operations of addition, subtraction, multiplication and division with their usual properties (e.g. distribution). One example of finite fields is GF(5) (also noted $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{F}_5$), the field of integers modulo 5. Indeed, in this field, one can:

- Add two elements: $4 + 3 \equiv 2 \mod 5$
- Subtract two elements: $2 - 3 \equiv 4 \mod 5$
- Multiply two elements: $3 \cdot 2 \equiv 1 \mod 5$
- Divide one element by another (where division is seen as multiplication by an inverse): $4/2 = 4 \cdot 2^{-1} = 4 \cdot 3 \equiv 2 \mod 5$

For any $n \in \mathbb{Z}$, the three first operations do exists in $\mathbb{Z}/n\mathbb{Z}$ and those structures are called rings. Division is fully defined when all nonzero elements have an inverse, which is only the case when n is prime. Actually, all the finite fields have p^i elements for a prime p and the particular case of prime order fields (when $i = 0$) are (isomorphic to) the $\mathbb{Z}/p\mathbb{Z}$ and are written GF(p) or $\mathbb{F}_p$. To construct finite fields of nonprime orders p^i for $i \neq 0$, one has to work with polynomials over GF(p) with operations modulo an irreducible polynomials of degree i.
In the following, we will construct the field GF(256=2^8).

1 The polynomial ring GF(2)[X]

We start with GF(2) which is simply the set $\{0, 1\}$ with addition and multiplication modulo 2. Those two operations can alternatively seen as the logical XOR and AND operations.

Addition in $\mathrm{GF}(2)$	**Multiplication in** $\mathrm{GF}(2)$
$0+0=0$	$0\cdot 0=0$
$0+1=1$	$0\cdot 1=0$
$1+0=1$	$1\cdot 0=0$
$1+1=0$	$1\cdot 1=1$

We then construct $\mathrm{GF}(2)[X]$ which is the ring of polynomials with coefficients in $\mathrm{GF}(2)$. An example of an element of this ring is $X^{15}+X^3+X^1+X^0 \in \mathrm{GF}(2)[X]$.

Encoding

Such polynomials can be represented as a binary string by concatenating all coefficients (which are in $\{0,1\}$). This binary string can subsequently be encoded in hexadecimal for a compact representation. For example $X^6+X^4+X+1 = 1X^6+0X^5+1X^4+0X^3+0X^2+1X+1$ can be written `1010011` in binary and `0x53` in hexadecimal.

Addition/subtraction

Addition and subtraction are performed coefficient-wise on the polynomials in the field $\mathrm{GF}(2)$.
For example, X^3+X^2+1 added to X^2+X+1 is:

$$(1X^3+1X^2+0X+1)+(0X^3+1X^2+1X+1) = (1+0)X^3+(1+1)X^2+(0+1)X+(1+1) = X^3+X.$$

Alternatively, this can be written `0xD + 0x7 = 0xA` $\in \mathrm{GF}(2)[X]$

Multiplication

Multiplication is the usual polynomial multiplication except that coefficients are reduced modulo 2. For example, (X^2+X) multiplied by (X^6+1) is:

$$(X^2\cdot X^6)+(X\cdot X^6)+(X^2\cdot 1)+(X\cdot 1) = X^8+X^7+X^2+X.$$

Alternatively, this can be written `0x6 · 0x41 = 0x186` $\in \mathrm{GF}(2)[X]$

Modular reduction of polynomials

For a given polynomial $m(X)$. A polynomial $a(X)$ can always be written:

$$a(X) = b(X)m(X) + r(X),$$

where the degree of $r(X)$ is less than the degree of $m(X)$. Then, we can say that $a(X)$ is congruent to $r(X)$ modulo $m(X)$, and write it

$$r(X) \equiv a(X) \mod m(X).$$

To reduce $a(X)$ modulo $m(X)$, the simplest procedure is to repeatedly add or subtract a multiple of $m(X)$ to make the highest degree term disappear until obtaining a polynomial of degree less than the degree of $m(X)$.

Exercices

Exercice 1. Write the polynomial corresponding to `0x7A` in hexadecimal.

Solution. $X^6 + X^5 + X^4 + X^3 + X$

Exercice 2. What is the hexadecimal representation of $X^7 + X^6 + X^2 + 1$?

Solution. `0xC5`

Exercice 3. Add $X^4 + X^3 + 1$ with $X^7 + X^4 + X^2 + 1$ in $\mathrm{GF}(2)[X]$. Rewrite the addition in hexadecimal representation. Which well-known operation has actually been performed between the hexadecimal values?

Solution. $X^7 + X^3 + X^2$
`0x19` + `0x95` = `0x8C` (XOR)

Exercice 4. Multiply $X^3 + X^2$ with $X^{17} + X^{16} + X + 1$.

Solution. $X^{20} + X^{18} + X^4 + X^2$

Exercice 5. Let $m(X) = X^8 + X^4 + X^3 + X + 1$. Reduce the following polynomials modulo $m(X)$:

1. $X^8 + X^7 + X^3 + 1$
2. $X^{10} + X^9 + X^8$
3. $X^{108} + X^{104} + X^{103} + X^{101} + X^{100}$

Solution.

1. $X^7 + X^4 + X$
2. $X^6 + 1$
3. 0

2 $\mathrm{GF}(2^8)$: finite field of order 256

There exists multiple ways to construct $\mathrm{GF}(2^8)$. The one we are using in this document was not randomly chosen, we follow the construction used to define the algorithm Rijndael (AES).

Here, the field $\mathrm{GF}(2^8)$ is defined as the set of binary polynomials of degree less than 8. Addition is identical to the one in $\mathrm{GF}(2)[X]$ because the result of the addition of two polynomials of degree less than 8 is also of degree less than 8. Unlike addition, the multiplication between two degree less than 8 polynomials results in polynomials of degrees up to 14. Hence, we shall reduce modulo a degree 8 polynomials. In particular, we will reduce modulo an irreducible polynomials to get the field structure.

2.1 Multiplication

Let $m(X) = X^8 + X^4 + X^3 + X + 1$ be the irreducible polynomial used in Rijndael. In this representation of $\mathrm{GF}(2^8)$, multiplying two polynomials $a(X)$ and $b(X)$ is done by:

- First multiplying in $\mathrm{GF}(2)[X]$
- Then reduce the result modulo $m(X)$.

2.2 Multiplicative inverse

As explained in the intro, the term *field* indicates that we are working with an object with specific algebraic properties. In particular, addition and multiplication should be invertible. For example, the reals numbers with addition and multiplication form a field. Every element has an additive inverse ($a + (-a) = 0, \forall a \in \mathbb{R}$), and every nonzero element has a multiplicative inverse ($a \cdot \frac{1}{a} = a \cdot a^{-1} = 1, \forall a \in \mathbb{R} \setminus \{0\}$).

Inverting addition in GF(2^8) is trivial because elements are self inverse: $a + a = 0$, for all a.

For multiplication, every element except 0 has an inverse. For any polynomial $a \in$ GF(2^8), $a \neq 0$, there always exist another polynomial a^{-1} such that $a \times a^{-1} = a^{-1} \times a = 1$.

2.3 Exercices

Exercice 7. Multiplication by X. Perform the following multiplication in GF(2^8):

1. $X \cdot X^3$
2. $X \cdot (X^6 + X^2 + 1)$
3. $X \cdot X^7$, then $X \cdot (X \cdot X^7)$
4. $X \cdot (X^7 + X^3 + X^2 + 1)$

Solution.

1. X^4
2. $X^7 + X^3 + 1$
3. $X \cdot X^7 \equiv X^4 + X^3 + X + 1$ and $X \cdot X \cdot X^7 \equiv X^5 + X^4 + X^2 + X$
4. 1

Exercice 8. Using results of the last exercise, compute $(X^2 + X + 1)X^7$.

Solution. $X^7 + X^5 + X^3 + X^2 + 1$

Exercice 9. Multiply `0x8A` by `0xD5`.

Solution. $X^7 + X^6 + X^5 + X^4 + X^3 + X$

Exercice 10. Compute X^{-1}, that is the say the inverse of X. Explain how to compute the inverse of X^2.

Solution. $X^{-1} \equiv X^7 + X^3 + X^2 + 1$
$X^{-2} \equiv X^7 + X^6 + X^3 + X + 1$

2.4 Extra exercice (harder)

The following exercice has been exctracted from the following book: Baigneres, Th., Junod, P., Lu, Y., Monnerat, J., Vaudenay, S., "A Classical Introduction to Cryptography Exercise Book" (2006)

In AES, the main diffusion step is a linear application defined as follows. The 32-bit blocks are considered as polynomials of degree smaller than 4 over GF(256). This linea application consists in multiplying the input polynomial $A(Y) = a_3 \cdot Y^3 + a_2 \cdot Y^2 + a_1 \cdot Y + a_0$ with the fixed polynomial $C \in$GF(256)$[Y]$ = 0x03 $\cdot Y^3 +$ 0x01 $\cdot Y^2 +$ 0x01 $\cdot Y +$ 0x02 modulo the polynomial $Y^4 + 1$ defined in GF(256)$[Y]$ as well.
Compute the image of 0x836F13DD (where $a_0 =$ 0x83, $a_1 =$ 0x6F, $a_2 =$ 0x13, $a_3 =$ 0xDD under this diffusion step.
(Hint: computing modulo $Y^4 + 1$ means $Y^4 + 1 \equiv 0$ and $1 \equiv -1 \mod 2$)