Introduction to Cryptography

Alvin Lin

January 2018 - May 2018

Polynomial Arithmetic

Finite Fields of the Form $GF(p^m)$

Galois' Theorem: An order-n finite field exists if and only if $n = p^m$ for some prime p and some positive integer m.

- p is called the characteristic of this finite field.
- The order of a finite field is its number of elements.
- We use $GF(p^m)$ or $\mathbb{F}_{p^m}$ to represent the finite field of order p^m.
- An order-n finite field is unique (up to isomorphism).
- Addition and multiplication module a prime number p form a finite field $\mathbb{Z}_p = GF(p)$.
- If $m = 1$, then $\mathbb{Z}_p = GF(p)$
- One way to construct a finite field with $m > 1$ is using the polynomial basis. The field is constructed as a set of p^m polynomials along with two polynomial operations.

Polynomial Arithmetic

A polynomial $f(x)$ is a mathematical expression of the form:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

The highest exponent of x is the degree of the polynomial. $a_n, a_{n-1}, \ldots, a_0$ are called coefficients. We can add, subtract, multiply, and divide polynomials. AES is a byte oriented cipher where 1 byte can be represented as a 7th degree polynomial.

All arithmetic can be done in the Galois field $GF(2^8)$. If a polynomial is divisible only by itself and constants, then we call this polynomial an irreducible polynomial. $gcd(a(x), b(x))$ is the polynomial of maximum degree that divides both $a(x)$ and $b(x)$. Similar to integers, you can do modular arithmetic with polynomials over a field. Now the operands and modulus are polynomials.

Polynomial Arithmetic Modulo $(x^3 + x + 1)$

Over addition:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Over multiplication:

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech