Crypto Notes

Jaelyn McCracken

Septemer 26th, 2023

1 Finite Fields

Goal: Find fields with 2^k elements ($\mathbb{F}_{2^k}$).

- AES uses $\mathbb{F}_{256}$
- Find $\mathbb{F}_4 \neq 2_4$ (not a field).
- Trick: use polynomials $\mathbb{F}_2[x]$
    - polynomials whose coefficients are 0,1 in $\mathbb{F}_2$
- Can do division with remainder has degree smaller (not the same) than thing you're dividing by.

1.1 Warm up

What is $x^5 + x^2 + 1(modx^3 + x)$?

$$
\begin{array}{r|l}
 & x^2 + 1 \;\; R(x^2 + x + 1) \\
\hline
x^3 + x & x^5 + x^2 + 1 \\
 & -\;(x^5 + x^3) \\
\hline
 & x^3 + x^2 + 1 \\
 & -\;(x^3 + x) \\
\hline
 & x^2 + x + 1
\end{array}
$$

Answer: $x^5 + x^2 + 1 \equiv x^2 + x + 1(\text{mod } x^3 + x)$

1.2 Irreducible

- If f(x) has degree k (f(x)= x^k+...) how many remainders are there? 2^k
- To get a field our modulus needs to not be factorable into smaller polynomials. These polynomials are called irreducible (Think like prime but for polynomials)
- If f(x) is irredicuble in $\mathbb{F}_2[x]$ then the polynomials (mod f(x)) are a field.

- To find $\mathbb{F}_{2^k}$ need an irredicuble polynomial of degree k.

Find $\mathbb{F}_4 = \mathbb{F}_{2^k}$ (need irreducible polynomial of degree 2).
Possible degree of 2 polynomials.
$x^2 = x * x$: (not irredicuble)
$x^2 + x = x(x+1)$: (not irredicuble)
$x^2 + 1$: (not irredicuble)
$x^2 + x + 1$: (irredicuble!!!)

- $\mathbb{F}_4$ is polynomials in $\mathbb{F}_2[x]$ (mod $x^2 + x + 1$)
- $\mathbb{F}_4$= {0,1,x,x+1}

1.3 Addition/multiplication tables (mod $x^2 + x + 1$)

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$*$	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Light blue= Field!

1.4 Uses

- AES uses $\mathbb{F}_{256} = \mathbb{F}_{2^4}$.
- SAES uses $\mathbb{F}_{16} = \mathbb{F}_{2^4}$.

1.5 Example

Pick x^4+x+1 as our degree 4 irredicuble polynomial for $\mathbb{F}_{16}$ $\mathbb{F}_{16}$ is polynomials modulo $x^4 + x + 1$

Ex: Multiply $(x^3 + 1)(x^2 + x)$ in $\mathbb{F}_{16}$.
$(x^3 + 1)(x^2 + x) = x^5 + x^4 + x^2 + x$.

$$
\begin{array}{r}
x+1 \;\; R(x+1) \\
x^4+x+1 \overline{\big) \, x^5 + x^4 + x^2 + x} \\
\underline{- \quad (x^5 + x^2 + x) } \\
x^4 \\
\underline{- \quad (x^4 + x + 1)} \\
x+1
\end{array}
$$

Answer: $x^5 + x^4 + x^2 + x \equiv x + 1 \pmod{x^4 + x + 1}$

1.6 Euclid's Algorithm

Euclid's Algorithm work identically for polynomials as integers. Find $(x^2)^{-1}$ (mod $x^4 + x + 1$)

- Find GCD (a,m)=1
- $x^4 + x + 1 = (x^2)(x^2) + (x + 1)$

$$\begin{array}{r} x^2 \;\; R(x+1) \\ x^2 \overline{\big) x^4 + x + 1} \\ - \;\; (x^4) \\ \hline x + 1 \end{array}$$

$$\begin{array}{r} x + 1 \;\; R(1) \\ x + 1 \overline{\big) x^2} \\ - \;\; (x^2 + x) \\ \hline x \\ - \;\; (x + 1) \\ \hline 1 \end{array}$$

- Keep track of x^2 and $x^4 + x + 1$.
- Backwards

  $1 \equiv x^2 + (x + 1)(x + 1)$

  $x + 1 \equiv (x^4 + x + 1) + (x^2)(x^2)$

  $1 \equiv x^2 + (x + 1)((x^4 + x + 1) + (x^2)(x^2))$

  $1 \equiv 1x^2 + (x + 1)(x^4 + x + 1) + (x^3 + x^2)(x^2)$

  $1 \equiv (x^3 + x^2 + 1)(x^2) + (x + 1)(x^4 + x + 1)$ Linear Combination

  $1 \equiv (x^3 + x^2 + 1)(x^2) + (x + 1)(x^4 + x + 1) \pmod{x^4 + x + 1}$

  $1 \equiv (x^3 + x^2 + 1)(x^2) \pmod{x^4 + x + 1}$

  $(x^2)^{-1} \equiv (x^3 + x^2 + 1) \pmod{x^4 + x + 1}$