Cryptography 2/14

Reagan Shirk

February 14, 2020

Polynomials over Finite Fields

- Something about being hardware friendly
- What is a finite field?
  - $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$
  - $\mathbb{F}_2 = \{0, 1\}$
  - $\mathbb{F}_2[x] = \{$polynomials in x with coefficients in $\mathbb{F}_2\}$
- Addition is very easy

$$\begin{aligned}(x^2 + x) + (x^3 + x) &= x^3 + x^2 \\ &\Rightarrow \text{ easy}\end{aligned}$$

- Multiplication is also easy?

$$\begin{aligned}(x + 1)^2 &= x^2 + 1 \\ \Rightarrow \text{ for the above ring only } (\mathbb{F}_2[x])\end{aligned}$$

How do we do the below multiplication?

$$(x^3 + x + 1) \times (x^2 + x)$$
$$x^3 + x + 1 :$$

$$\begin{array}{r} 1011 \\ 110 \\ \hline 0000 \\ 1011 \\ 1011 \\ \hline 111010 \rightarrow x^5 + x^4 + x^3 + x \end{array}$$

- Division with Remainder

$$\frac{x^4 + 1}{x^4 + x^2 + 1}$$
$$\text{Quotient: } 1$$
$$\text{Remainder: } x^2$$

- Irreducible Polynomial
  - Can you take a polynomial and reduce it into at least 2 polynomials with a degree greater than zero? If no, the polynomial is irreducible
    - $x + 1$ is irreducible
    - $x^2 + 1 = (x + 1) \times (x + 1) \rightarrow$ not irredicible (or redicible to avoid the double negative)
  - Redicability depends on the coefficient ring, for example the reducible polynomial above is irreducible in $\mathbb{Z}[x]$