Corpos Finitos usados em Criptografia

Jaime Edmundo Apaza Rodriguez **Douglas Silva Maioli**
Depto de Matemática, FEIS, UNESP,
15385-000, Ilha Solteira, SP
E-mail: jaime@mat.feis.unesp.br, doug.mat@hotmail.com

RESUMO

Os métodos criptográficos, usando curvas elíticas, vem se tornando extremamente úteis nos últimos anos, exibindo maior segurança, confiabilidade e eficiência que outros métodos.

O objetivo desse trabalho é apresentar dois tipos de Corpos Finitos que são de interesse à Criptografia. Tal interesse se deve ao fato de que muitos padrões que especificam técnicas criptográficas baseadas em Curvas Elíticas se restringem a $\mathbb{F}_p$ ou $\mathbb{F}_{2^m}$.

1. Corpos Primos

Para p primo, considere o corpo $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$. Temos as seguintes operações aritméticas definidas em $\mathbb{F}_p$:

a) Adição módulo p: Se $a, b \in \mathbb{F}_p$, então $r = (a + b) mod\ p$, onde r é o resto da divisão de $a + b$ por p. Assim $0 \leq r < p$.

b) Multiplicação módulo p: Se $a, b \in \mathbb{F}_p$, então $r = ab(mod\ p)$.

c) Inversão módulo p: Se $a \in \mathbb{F}_p$, não-nulo, o inverso a^{-1} de a é o único inteiro c tal que $0 \leq c < p$ com $ac = 1(mod\ p)$.

Apesar de $\mathbb{F}_2$ satisfazer a definição acima, frequentemente $\mathbb{F}_p$ é chamado de *Corpo Primo* quando $p > 2$. Em especial, para aplicações criptográficas, p é geralmente um número de, pelo menos, 160 bits.

2. Corpos Binários

Consideremos o corpo $\mathbb{F}_{2^m}$. Seus elementos podem se representados como polinômios de grau $m-1$, com coeficientes em $\{0, 1\}$ (*base polinomial*).

Considere $f(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + 1$, com $f_i \in \{0, 1\}$, um polinômio irredutível de grau m. Desta forma definimos:

$$\begin{aligned}\mathbb{F}_{2^m} &= \{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \\ &\cdots + a_2x^2 + a_1x + a_0 : a_i \in \{0, 1\}\}.\end{aligned}$$

Assim, para $A, B, C \in \mathbb{F}_{2^m}$, temos:

$A = a_{m-1}z^{m-1} + \cdots + a_2z^2 + a_1z + a_0,$

$B = b_{m-1}z^{m-1} + \cdots + b_2z^2 + b_1z + b_0,$

$C = c_{m-1}z^{m-1} + \cdots + c_2z^2 + c_1z + c_0.$

Então as operações aritméticas definidas sobre $\mathbb{F}_{2^m}$, usando bases polinomiais, são:

1) Adição módulo $f(x)$: $A + B = C$, onde $c_i = a_i + b_i\ (mod\ 2)$. (*Computacionalmente, isto equivale a um ou exclusivo dos bits* a_i *e* b_i).

2) Multiplicação módulo $f(x)$: $A \times B = R$, onde R é o resto obtido quando dividimos o polinômio $A \cdot B$ por $f(x)$.

3) Inversão módulo $f(x)$: Se A é um elemento não nulo de $\mathbb{F}_{2^m}$, o inverso de A, denotado por A^{-1}, é o único elemento $C \in \mathbb{F}_{2^m}$, tal que $A \times C = 1$.

Uma outra forma de representar os elementos de $\mathbb{F}_{2^m}$ é usar *bases normais*. Uma base normal de $\mathbb{F}_{2^m}$, sobre $\mathbb{F}_2$, é da forma $\{\alpha, \alpha^{2^i}, \cdots, \alpha^{2^{m-1}}\}$, onde $\alpha \in \mathbb{F}_{2^m}$. Tal base sempre existe e todo elemento $a \in \mathbb{F}_{2^m}$ pode ser escrito na forma

$$a = \sum_{i=0}^{m-1} a_i\alpha^{2^i}, \quad \text{onde} \quad a_i \in \{0, 1\}.$$

Referências

[1] R. A. Miranda, Criptossistemas Baseados em Curvas Elíticas, Dissertação de Mestrado, IC, UNICAMP, 2002.

[2] A. J. de Almeida Júnior, Criptossistemas Baseados em Curvas Elíticas: Estudo de casos e implementação em processador de sinais digitais, FEEC, UNICAMP, 2002.