Raízes primitivas e aplicações em criptografia

Roberta A. do N. Ribeiro[1] **& Grasiele C. Jorge**[2]

[1]Universidade Estadual Paulista - Câmpus Guaratinguetá

[2]Instituto de Ciência e Tecnologia - Universidade Federal de São Paulo

roberta.ribeiro@unesp.br, grasiele.jorge@unifesp.br

Introdução

Neste trabalho serão abordados os conceitos de raízes primitivas, logaritmos discretos e o algoritmo de criptografia ElGamal.

Raízes primitivas

Definição 1. *Se n é um inteiro positivo, a* ***função ϕ de Euler****, denotada por $\phi(n)$, é definida como sendo o número de inteiro positivos menores do que ou iguais a n que são relativamente primos com n.*

Teorema 1. *[4, 5]* **Teorema de Euler** *- Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \,(mod\, m).$$

Definição 2. *Seja $a \in \mathbb{Z}$, tal que $(a, m) = 1$. O menor inteiro positivo k para o qual $a^k \equiv 1 \,(mod\, m)$ é chamado* ***ordem de a módulo m*** *e é denotado por $ord_m a$. Se $ord_m a = \phi(m)$ dizemos que a é uma* ***raiz primitiva*** *módulo m.*

Exemplo 1. *Considerando as potências de 4 módulo 7, temos $4^1 = 4 \equiv 4 \,(mod\, 7)$, $4^2 = 16 \equiv 2 \,(mod\, 7)$ e $4^3 = 64 \equiv 1 \,(mod\, 7)$. Logo, $ord_7 4 = 3$. Agora, considerando as potências de 5 módulo 7, temos $5^1 = 5 \equiv 5 \,(mod\, 7)$, $5^2 \equiv 4 \,(mod\, 7)$, $5^3 \equiv 6 \,(mod\, 7)$, $5^4 \equiv 2 \,(mod\, 7)$, $5^5 \equiv 3 \,(mod\, 7)$ e $5^6 \equiv 1 \,(mod\, 7)$ Logo, $ord_7 5 = 6 = \phi(7)$ e portanto 5 é uma raiz primitiva módulo 7.*

Teorema 2. *[4, 5] Se um inteiro $m \geq 1$ não é da forma $1, 2, 4, p^t$ e $2p^t$ (p primo ímpar), então m não possui raiz primitiva.*

Observação 1. *Um inteiro a é uma raiz primitiva módulo m se, e somente se, a é um gerador do grupo $\mathbb{Z}_m^*$, onde*

$$\mathbb{Z}_m^* = \left\{\overline{b} \in \mathbb{Z}_m;\ \overline{b} \text{ é invertível}\right\}.$$

Neste caso, $(\mathbb{Z}_m^*, \cdot)$ é um grupo cíclico.

Logaritmo discreto

Sejam p um número inteiro primo e a uma raiz primitiva módulo p. Para todo inteiro b, tal que p não divide b, existe um único inteiro $j, 0 \leq j < p - 1$, tal que

$$b \equiv a^j \,(mod\, p).$$

Denotamos j por $dlog_{a,p}(b)$ e o chamamos **índice do inteiro b na base a módulo p**. Portanto, $dlog_{a,p}(b)$ é o menor inteiro maior ou igual a zero, tal que:

$$a^{dlog_{a,p}(b)} \equiv b \,(mod\, p).$$

Proposição 1. *[3] Dados a uma raiz primitiva módulo p e $x, y \in \mathbb{Z}$, tais que $p \nmid x$ e $p \nmid y$, valem as seguintes propriedades:*

- $dlog_{a,p}(1) = 0$
- $dlog_{a,p}(a) = 1$
- $dlog_{a,p}(xy) \equiv dlog_{a,p}(x) + dlog_{a,p}(y) \,(mod\,(p-1))$
- $dlog_{a,p}(x^r) \equiv r \cdot dlog_{a,p}(x) \,(mod\,(p-1))$.

Definição 3. *A função $dlog_{a,p}(x) : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_{p-1}$ é chamada* ***logaritmo discreto de base a módulo p****.*

O problema do logaritmo discreto

Fixada a uma raiz primitiva módulo p e dado $\overline{b} \in \mathbb{Z}_p^*$, o problema do logaritmo discreto consiste em encontrar $x, 0 \leq x \leq (p-2)$, tal que $b \equiv a^x \,(mod\, p)$.

Nenhum algoritmo clássico eficiente para computar logaritmo discreto de maneira geral $dlog_{a,p}(x)$ é conhecido até o momento.

O algoritmo criptográfico ElGamal

Suponha que Alice deseja enviar uma mensagem para Beto. Para iniciar o processo, Beto deve criar uma chave pública, seguindo os passos a seguir:

- Beto escolhe um primo p e um gerador α de $\mathbb{Z}_p^*$.
- Beto escolhe uma chave privada x_j, $1 < x_j < p - 1$ e calcula $y_j = \alpha^{x_j} \,(mod\, p)$.
- A chave pública de Beto será (p, α, y_j).

Para cifrar a mensagem M, Alice utiliza a chave pública de Beto (p, α, y_j) e realiza os passos a seguir:

- Alice escolhe um número inteiro $x_m, 0 < x_m < p - 1$ e calcula:

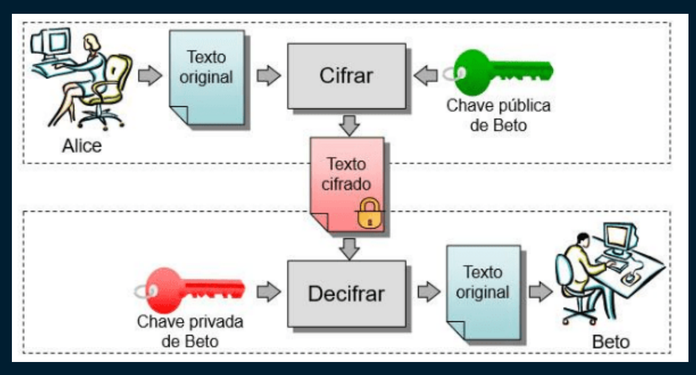
$$c_1 \equiv \alpha^{x_m} \,(mod\, p) \quad \text{e} \quad c_2 \equiv M y_j^{x_m} \,(mod\, p).$$

- Alice envia para Beto a mensagem encriptada (c_1, c_2).

Para decifrar a mensagem, Beto utiliza (c_1, c_2) e aplica os passos a seguir:

- Beto calcula $(y_j^{x_m})^{-1} \equiv c_1^{p-1-x_j} \,(mod\, p)$.

  De fato, $c_1^{p-1-x_j} \equiv c_1^{p-1} c_1^{-x_j} \equiv 1 \cdot (\alpha^{x_m})^{-x_j} \equiv (\alpha^{x_j})^{-x_m} \equiv (y_j^{x_m})^{-1} \,(mod\, p)$.
- Beto obtém M da relação $M \equiv c_2 (y_j^{x_m})^{-1} \,(mod\, p)$.



Referências

[1] S. C. Coutinho. *Números Inteiros e Criptografia RSA*. Coleção Matemática e Aplicações. Rio de Janeiro: IMPA, 2^a edição, 2014.

[2] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, pages 473 – 481, 1984.

[3] L. M. Figueiredo. *Introdução à Criptografia*. Fundação CECIERJ. Rio de Janeiro: UFF/CEP-EB, vol. 2, 2010.

[4] F. B. Martinez, C. G. Moreira, N. Saldanha e E. Tengan. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides. Rio de Janeiro: IMPA, 4^a edição, 2015.

[5] J. P. O. Santos. *Introdução à Teoria dos Números*. Coleção Matemática Universitária: IMPA, 3^a edição, 2015.

Agradecimentos

PICME

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico