O Protocolo Diffie-Hellman Sobre Curvas Elípticas

Jaime Edmundo Apaza Rodriguez
Departamento de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
E-mail: jaime@mat.feis.unesp.br

Douglas Silva Maioli
Departamento de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
E-mail: douglasmaioli@bol.com.br

Divane Aparecida de Moraes Dantas
Departamento de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
E-mail: di-dantas@hotmail.com

RESUMO

A primeira prática da criptografia assimétrica foi proposta por Whitfield Diffie e Martin E. Hellman no trabalho "*New directions in Cryptography*" publicado em 1976, que chamaram de Troca de chaves ou Protocolo Diffie-Hellman. Porém este não é um método para cifrar mensagens e tal algoritmo foi arquitetado para que dois usuários estabelecessem uma chave simétrica através de um canal de comunicação inseguro. Sua segurança está baseada diretamente na dificuldade de se resolver o Problema do Logaritmo Discreto (PLD) em grupos cíclicos.

Dado que o conjunto de pontos de uma curva elíptica formam um grupo abeliano, então podemos usar um problema análogo ao PLD, que chamaremos de Problema do Logaritmo Discreto de uma Curva Elítica (PLDCE). Assim, quando trabalhamos com uma curva elíptica E, a dificuldade está em, conhecendo um par de pontos P e Q em E, determinar um inteiro k tal que P = kQ.

A principal diferença da idéia original e da forma que mostraremos aqui é que essa troca de chave utilizará pontos sobre uma curva elíptica, ao invés de grupos cíclicos, o que poderá nos trazer uma maior segurança, pela falta de algoritmos sub-exponenciais que dividem dois pontos de uma curva elíptica, e pela crença de que o PLDCE é significativamente mais difícil que o PLD. Um fator negativo de se utilizar curvas elípticas na criptografia, é por não estar demonstrado ainda que o PLDCE é mais seguro que os outros métodos, apesar da grande quantidades de evidências que nos levam a crer nesta hipótese.

Vamos mostrar então de um modo geral como duas pessoas, que chamaremos de Alice e Bob, trocam uma chave de um sistema simétrico, através do protocolo Diffie-Hellman sobre uma Curva Elíptica:

I. Alice e Bob escolhem publicamente uma curva elíptica E, e um ponto P pertencente a E.
II. Bob escolhe um inteiro B, que será sua chave privada e calcula S=PB.
III. Da mesma forma Alice escolhe um inteiro A para ser sua chave privada e calcula T=PA.
IV. Bob envia S a Alice.
V. E ela retribui enviando T para Bob.
VI. Bob calcula TB=PAB=U.
VII. Alice calcula SA=PBA=PAB=U.

No final do processo Bob e Alice possuem a mesma chave U, e podem trocar mensagens através de um sistema criptográfico simétrico, utilizando esta chave.

Para facilitar a compreensão, retiramos um exemplo de [2], no qual Bob e Alice se utilizam da curva elíptica $E:y^2=x^3+101x+552$ sobre o corpo primo finito Z_{4229} , sabendo que 4229 é um número primo, e o ponto P=(4197,231) que pertence a $E(Z_{4229})$, o conjunto de pontos da curva elíptica. Os outros passos que eles realizam são:

II. Bob escolhe o inteiro B=1402 que será sua chave privada e envia a Alice S=PB=(4197,231)1402=(392,2766).
III. Alice escolhe o inteiro A=1011 que será sua chave privada e envia a Bob T=PA=(4197,231)1011=(3617,263).
VI. Bob calcula TB=(3617,263)1402=(3990,3565).
VII. Alice calcula SA=(392,2766)1011=(3990,3565).

Assim, tanto Alice, quanto Bob, possuem uma chave particular U=(3990,3565) em comum transmitida em segurança, pois, para que algum usuário que interceptou as mensagens de Bob e Alice, descubra a chave U=(3990,3565), este deve dividir S=(392,2766) por P=(4197,231), ou seja, encontrar o inteiro B tal que S=PB, que já sabemos que é B=1402, e assim calcular TB=U, porém a tarefa de encontrar B é muito difícil, e é nessa dificuldade, que como dissemos, a segurança do método está baseada, com essa chave em comum nas mãos, eles já podem utilizar algum método criptográfico simétrico.

Através desse processo podemos resolver um grande problema da Criptografia Simétrica, que é realizar a troca de chaves de uma forma fácil, rápida e segura, ao mesmo tempo. Temos também que essa troca de chaves é feita através de um método assimétrico, porém para transmitir apenas uma chave simétrica e, portanto, menos custoso que os métodos assimétricos para transmitir mensagens. Dessa forma, essa é uma ótima alternativa, dentro dos Métodos Criptográficos, pois os Métodos Assimétricos para troca de mensagens necessitam de um poder computacional muito alto, e os Simétricos possuem esse grande "defeito", que é a necessidade de trocar informações (as chaves) por meio de redes inseguras. Com esse protocolo que une os dois métodos, podemos realizar essa troca de chaves de modo seguro, utilizando ainda algum método Simétrico, não necessitando, assim, de um grande poder computacional.

Palavras-chave*: Curvas Elípticas, Troca de chaves, Sistemas Criptográficos*

Referências:

[1] A. M. Rogério, Criptossistemas Baseados em Curvas Elípticas, Dissertação de Mestrado, UNICAMP, 2002.

[2] C. da S. L. Pedro, B. de O. Fábio, Criptografia com Curvas Elípticas sobre Corpos Finitos, Laboratório Nacional de Computação Científica, LNCC.

[3] D. Whitfield, E. H. Martin, New directions in Cryptography, *IEEE Transactions on Information Theory*, 1976.

[4] N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, 1994.

[5] P. Marcos, Critpografia com curvas elipticas, Dissertação de Mestrado, Universidade Salvador, Bahia, 2005.

[6] U. Nelson, R. J. David, A survey of Cryptography Libraries Suporting Elliptic Curves Crytpography, Terceiro Congresso Iberoamericano de Seguridade Informatica, p. 159-176, Chile, 2005.

[7] N. Klobitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol. 48, Number 177, p. 203-209, 1987.

[8] A. V. Mendes, Estudo de Criptografia com Chave Pública baseada em Curvas Elípticas, Monografia Depto de Ciências, Montes Claros, 2007.