Geração de expressões pseudoaleatórias

Este passo consiste na geração através de um algoritmo pré-definido de expressões matemáticas baseada numa dada chave pública de acordo com a posição da chave privada que se deseja.

Por exemplo:

Chave pública: **(65 bytes)**

04CDDCE816EF153B8E8EADECE2A6489481B7332FD99A4718066C40B1B688F6A08828241A5CC0A97E2C916C2EC610838325FB49403BB3ED352BB4574776FEC5E3B3, **ou seja:**

X = CDDCE816EF153B8E8EADECE2A6489481B7332FD99A4718066C40B1B688F6A088

Y = 28241A5CC0A97E2C916C2EC610838325FB49403BB3ED352BB4574776FEC5E3B3

Chave privada: **(32 bytes)**

375D75D0A1188016E9DE9395BFF6334BD3FDCEB5884766CE87454DB30612D936

Obter o valor da chave privada na posição 0 (0x37):

Após **513** tentativas é gerada a seguinte expressão:

(Y[12] ^ Y[12]) * (Y[18] ^ Y[26]) + (Y[6] | Y[14]) % (X[13] | X[31]), substituindo os valores e calculando o resultado da expressão, temos como resultado **55** ou **0x37 (valor correto da chave privada na posição 0).**

Agora, vamos tentar gerar a expressão que leve ao valor da chave privada na posição **1:**

Após **270** tentativas é gerada a seguinte expressão:

(X[18] % Y[23]) | (~Y[10] * X[0]), substituindo os valores e calculando o resultado da expressão, temos como resultado **93** ou **0x5D (valor correto da chave privada na posição 1).**

O algoritmo tem **3 valores de entrada:** Chave pública **(X e Y)**, Posição da chave privada que deseja-se descobrir **(0-31)** e tentativa **(0-2^{64}).**

Utilizando a chave pública acima como exemplo (conhecendo o valor correto da chave privada), teremos como resultado: [513, 270, 151, 500, 546, 176, 305, 823, 369, 1310,

751, 792, 30, 61, 464, 3419, 1091, 84, 780, 52, 313, 112, 447, 52, 265, 10, 333, 775, 622, 2, 92, 2], cada valor refere-se a tentativa na qual foi gerada a expressão que resultou no valor correto da chave privada na sua respectiva posição.