Criptografia ECC Simplificada

Nome do arquivo: ecc.c

Implementar um sistema criptográfico baseado em ECC- Elliptic Curve Cryptography que utilize um tamanho de chave menor que os suportados pelas bibliotecas criptográficas disponíveis.

As operações aritméticas realizadas pelo algoritmo ocorrem sobre pontos da curva elíptica definida. O conjunto de pontos válidos para o algoritmo é dado por um conjunto finito de pontos sobre a curva mais um ponto no infinito, neste caso definido por O=(0,0). Para este conjunto de pontos é definida a operação de soma tal que:

Seja P, Q e G pontos quaisquer da curva e O (ponto no infinito), valem as propriedades:

- P = Q + G é um ponto da curva.
- Q + G = G + Q
- P + Q + G = (P + Q) + G = P + (Q + G)
- O é o elemento neutro da adição: Q + O = O + Q = Q
- Existe o inverso aditivo G = -Q tal que Q + G = G + Q = O

Sua equipe (dupla) deve implementar a operação de multiplicação de um ponto (G = (Xg,Yg)) da curva por um escalar (n), obtendo um outro ponto da curva (R = (Xr,Yr)). Esta operação é definida como a soma sucessiva do ponto G (gerador).

Exemplo: Se n = 3, então R = 3G = G + G + G

A soma de dois pontos quaisquer (Q e G) para a curva elíptica utilizada, resulta em outro ponto da curva (R = Q + G), sendo definida abaixo.

Considere,

- R= (Xr,Yr) , Q = (Xq,Yq), G =(Xg,Yg) e o ponto no infinito O = (0,0).
- que as coordenadas do ponto na curva (X,Y), o escalar n e todas as operações realizadas sobre estes operandos são operações sobre um corpo finito primo GF(Z_p). Ou seja, Xi,Yi e n são inteiros com $0 \leq$ Xi,Yi,n $\leq$ p-1, para qualquer coordenada ou escalar multiplicativo, e as operações são realizadas modulo um inteiro primo p, com $p < 10^7$.
- que se Q = (Xq,Yq), então –Q = (Xq,-Yq) mod p, ou seja, -Q = (Xq , (p-Yq) mod p) para $0 \leq$ Yq $\leq$ p-1.
- que nG = O para n = 0.

A operação de soma de pontos é definida por R = Q + G:

$$R = \begin{cases} (Xq,Yq) & \text{se } G = O \\ (Xg,Yg) & \text{se } Q = O \\ O & \text{se } Q = -G \text{ (ou } G = -Q) \\ (Xr,Yr) \text{ com } \lambda = (Yg - Yq) / (Xg-Xq) \bmod p & \text{se } Q \neq \pm G \text{ e } Q,G \neq O \\ (Xr,Yr) \text{ com } \lambda = (3Xq^2 + \mathbf{a}) / (2Yq) \bmod p & \text{se } Q = G \text{ e } Q,G \neq O \text{ e } Yq \neq 0 \end{cases}$$

$$Xr = (\lambda^2 - Xq - Xg) \bmod p$$

$$Yr = (\lambda (Xq - Xr) - Yq) \bmod p$$

Observação:

- **a** é um coeficiente da curva e será fornecido,
- o cálculo de λ é uma operação modular. Observe a divisão modular: X / Y = $X*(Y)^{-1}$. $(Y)^{-1}$ é o inteiro menor que p que multiplicado por Y resulta em (1 mod p), ou seja, Y * $(Y)^{-1}$ mod p = 1 mod p. Ex.: 7 * 2 mod 13 = 1 mod p, então 2 é o inverso multiplicativo de 7 e vice-versa.

Exemplo:

Dados: n = 3; a = 3; p = 13; G=(2,10)

R = 3 G = G + G + G = (G + G) + G

$\lambda = (3Xg^2 + a)/(2Yg) \bmod p = (3*4+3)/(2*10) \bmod 13 = 2/7 \bmod 13 = 2*2 \bmod 13 = 4$

$Xq = (\lambda^2 - Xg - Xg) \bmod p = (16-2-2) \bmod 13 = 12$

$Yq = (\lambda (Xg-Xq) - Yg) \bmod p = (4*(2-12)-10) \bmod 13 = (-50) \bmod 13 = 2$

Segue-se o mesmo raciocínio para obter R = (12,2) + G

$\lambda = (Yg-Yq)/(Xg-Xq) \bmod p = (10-2)/(2-12) \bmod 13 = 8/3 \bmod 13 = 8*9 \bmod 13 = 7$

$Xr = (\lambda^2 - Xq - Xg) \bmod p = (49-12-2) \bmod 13 = 9$

$Yr = (\lambda (Xq-Xr) - Yq) \bmod p = (7*(12-9)-2) \bmod 13 = 6$

Entrada

A entrada é composta por vários casos de teste. Cada caso de teste é composto por duas linhas. A primeira linha contém o escalar multiplicativo ***n***. A segunda linha contém quatro inteiros, separados por espaço, sendo na ordem o parâmetro da curva ***a***, o inteiro primo ***p*** e as coordenadas do ponto G, ***X*** e ***Y***. Os casos de teste terminam quando o valor **n** for igual a zero.

Saída

A saída deve fornecer em uma única linha as coordenadas ***X*** e ***Y*** do ponto R = nG para cada caso de teste.

Exemplo de entrada	Saída para exemplo de entrada
2 3 13 2 10 3 3 13 2 10 9 3 13 2 10 5 10 13 3 6 6 10 13 3 6 10 10 13 3 6 0	12 2 9 6 0 0 10 0 1 9 0 0