Trabajo Teoría

Curva Elíptica

20 de noviembre de 2019

Sofía Almeida Bruno
Pedro Manuel Flores Crespo
María Victoria Granados Pozo

Índice

1. Introducción

2. Curva Elíptica Criptográfica

Parámetros de dominio para los algoritmos (p, a, b, G, n, h) donde:

- p: primo
- a, b: Coeficientes de la curva elíptica, hay que elegirlos con cuidado para que el algoritmo sea seguro
- G: Generador del grupo
- n: Orden del grupo
- h: Cofactor del subgrupo

3. Algoritmos

3.1. ECDSA

Algoritmo de firma digital, Elliptic Curve Digital Signature Algorithm, es una variante del algoritmo DSA (Digital Signature Algortihm) aplicado a curvas elipticas. Trabaja con el hash del mensaje en lugar de con el propio mensaje. La elección de la función hash es importante, de esto dependerá la seguridad del sistema criptográfico. El hash del mensaje tendrá una longitud de n bit.

Imáginemos que Alice quiere firmar un mensaje con su llave privada (d_A), y la otra persona, Bob, quiere validad la firma con la llave pública de alice (H_A). Alice es la única que puede producir las firmas válidas, sin embargo todo el mundo que tenga su llave pública puede verificarlas.

Alice y Bob están usando los parámetros del dominio. El hash truncado lo denotaremos por z.

Algoritmo de firma del mensaje de Alice, a partir de k y z se genera la firma con la clave privada de Alice:

1. Tomamos un entero k de forma aleatorio en el conjunto { 1, ..., n-1}.
2. Calcular $P = kG$.
3. Calcular el número $r = x_P$.
4. Si r es 0 entonces se toma otro k y se intenta de nuevo.
5. Se calcula $s = k^{-1}(z + rd_A) \bmod n$ con k^{-1} el inverso multiplicativo de k módulo n.
6. Si s es 0 entonces se elige otro k y se vuelve al principio.

Al final obtendremos la firma que será la pareja (r, s)

Ahora entra el juego Bob que para validar la firma, a partir del mensaje firmado y de z con la clave pública de Alice