ECDSA

De Wikipedia, la enciclopedia libre

ECDSA. **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA. Existen dos tipos de curvas dependiendo del campo finito en el que se definan que pueden ser GF(P) o GF(2^m).

Primitivas sobre curvas elípticas

Existen dos primitivas básicas para puntos en curvas elípticas:

- Suma de puntos.
- Multiplicación escalar.

Proceso de firma y verificación

- **Generación de llaves**

1. Seleccione una curva elíptica *E*.
2. Seleccione un punto *P* (que pertenezca a *E*) de orden *n*.
3. Seleccione aleatoriamente un número *d* en el intervalo [1, *n - 1*].
4. Calcule *Q = dP*.
5. *d* será la llave privada.
6. *Q* será la llave pública.

- **Proceso de firma**

1. Seleccione un número *k* de forma aleatoria.
2. Calcule $kP = (x_1,y_1)$.
3. Calcule $r = x_1 \bmod n$. Si *r* = 0 regresa al primer paso. (En este paso x_1 es tratado como un entero).
4. Calcule $(k^{-1}) \bmod n$.
5. Calcule $s = k^{-1}(H(m) + dr) \bmod n$. Si *s = 0* regrese al primer paso. (*H(m)* es el hash del mensaje a firmar, calculado con el algoritmo SHA-1).
6. La firma del mensaje *m* son los números *r* y *s*.

- **Proceso de verificación**

1. Verifique que *r* y *s* estén dentro del rango [1,*n - 1*].
2. Calcule $w = s^{-1} \bmod n$.
3. Calcule $u_1 = H(m)w \bmod n$.
4. Calcule $u_2 = r \cdot w \bmod n$.
5. Calcule $u_1P + u_2Q = (x_0,y_0)$
6. Calcule $v = x_0 \bmod n$
7. La firma verifica si y solo si *v = r*

Obtenido de «http://es.wikipedia.org/w/index.php?title=ECDSA&oldid=66697028»

Categorías: Algoritmos criptográficos | Criptografía de curva elíptica | Siglas de informática

Esta página fue modificada por última vez el 6 mayo 2013, a las 07:13.

El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; podrían ser aplicables cláusulas adicionales. Léanse los términos de uso para más información.
Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.