Certificados de Seguridad (SSL)

Encriptamiento RSA y ECC

La encriptación de la información de los certificados puede ser mediante el algoritmo RSA o mediante ECC.

El encriptamiento RSA es un algoritmo de cifrado basado en la selección de dos números primos muy grandes que luego son multiplicados por un número mayor; por lo que identificar los dos números primos utilizados para cifrar la información resulta un verdadero reto.

El algoritmo ECC se propuso en 1985 como una alternativa aún más segura, la cual funciona seleccionando un número de una curva elíptica y luego multiplicarlo por otro número que resulta en un nuevo punto en esta, lo que permite utilizar claves más pequeñas con un grado aún superior de complejidad.

ID único: #1032
Autor: n/a
Última modificación: 2020-11-19 06:01