Nº: 1	
Título del Artículo	Extended DSA
Revista y/o evento	Journal of Discrete Mathematical Sciences and Cryptography
Año	2008
Autores	Chen-Yu Lee, Wei-Shen Lai
Universidad o institución	Department of Computer Science National Chiao Tung University
Referencia APA	Chen-Yu Lee & Wei-Shen Lai (2008) Extended DSA, Journal of Discrete Mathematical Sciences and ryptography, 11:5, 545-550, DOI: 10.1080/09720529.2008.10698206

Palabras clave
DSA

Resumen
Los autores proponen una versión más actualizada de DSA, llamada Extended DSA, la cual plantea a groso modo, que a diferencia de DSA, el cual usa 160 bits para la generación de su primo q (una de las variables para la generación de la clave), Extended DSA usará 256, 384 y 512, permitiendo entonces, una mejora para el algoritmo. Proponen cada una de estas variaciones con diferentes nombres en relación a su tamaño, es decir, que Extended DSA o DSA-2, lo podemos referir de acuerdo a su tamaño, tal y respectivamente como DSA-160 (algoritmo DSA original) y sus variaciones, DSA-256, DSA-384 y DSA-512. Estas diferencias desde 256 en adelante, por ejemplo, en la parte de la generación de la clave, además de los cinco pasos ordinarios, se compone de dos extra en donde se eligen un entero bajo ciertas condiciones y un tipo de acuerdo al DSA correspondiente. En la generación de números aleatorios también se varían los diferentes tipos de parámetros que comúnmente tiene como base, aumentando la cantidad y el tamaño también de estos según corresponda. Todos estos tipos de cambios y otros en relación a los números primos y algunos pasos para generar una firma digital, fueron posibles gracias a la implementación o cambio de SHA-2 en lugar de SHA-1 como funciones de hash criptográficas.

Herramientas utilizadas
SHA-1 SHA-2 DSA Estándares del NIST para la generación de un DSA.

Comentarios
El artículo propone una mejora del algoritmo, lo que conlleva a mejoras en la seguridad, puesto que al aumentar sus parámetros de generación de claves, estos serán más grandes y así será más difícil para las máquinas descifrarlos. Utilizan parámetros de referencia para su mejora muy sólidos, lo que da una validez del artículo muy veraz. Explica detalladamente cómo se debe llevar a cabo el cambio de DSA a Extended DSA

Valoración	4