full line of software

Encriptación con AES

El Advanced Encryption Standard (AES) es una para el cifrado de datos electrónicos, ha sido adoptado a nivel mundial por su gran fiabilidad y seguridad. Es el medio aceptado de cifrar la información digital, incluyendo datos financieros, de telecomunicaciones, gubernamentales y militares.

A finales de los noventa, la administración norteamericana, consciente de la vulnerabilidad del algoritmo de cifrado **DES** (Data Encryption Standard), que estaba siendo utilizado para proteger los datos confidenciales, hasta el momento, decidió realizar un exhaustivo estudio y un concurso, para encontrar un algoritmo totalmente seguro a largo plazo. Para sorpresa de todos, dicho concurso fue ganado de manera contundente por un algoritmo de origen europeo, frente a los presentados por empresas y universidades americanas, a pesar de numerosas presiones. Este algoritmo, ha sido posteriormente certificado y recomendado por prácticamente todos los organismos oficiales y no oficiales de seguridad y encriptación. El algoritmo, es el Rijndael, ahora más conocido por la denominación norteamericana, que proviene de su función en los estamentos oficiales de dicho país, Advanced Encryption Standard o **AES**.

El AES se convirtió rápidamente en un estándar universal para todas las plataformas, gracias a su altísima seguridad y a su alto rendimiento, el cual lo hace particularmente adecuado para la encriptación mediante software. El AES, permite un “bloque” de cifrado de tamaño variable de 128, 192 o 256 bits asociado a claves de los mismos tamaños. Esto quiere decir:

- 3.4 x 10^38 posibles claves de 128 bit
- 6.2 x 10^57 posibles claves de 192 bit
- 1.1 x 10^77 posibles claves de 256 bit

Asumiendo que una máquina recupera una clave **DES en un segundo** (probando 7.2 x 10^16 claves por segundo), t**ardaría aproximadamente 149000 de billones de años para romper una llave 128 bits AES.**

Nuestros productos pueden cifrar los ficheros ZIPs de mediante AES, la combinación de ambos algoritmos de cifrado y compresión se ha demostrado particularmente adecuada, aumentando aun más la seguridad, disminuyendo drásticamente el tamaño de los datos resultantes y simplificando la operativa al poder almacenar en un solo “recipiente” múltiples ficheros. Los datos así cifrados pueden ser descifrados y editados en otras plataformas, con cualquier aplicación compatible AES.