Cifrar y descifrar con AES desde PowerShell

Advanced Encryption Standard (AES)

También conocido como Rijndael (pronunciado «Rain Doll» en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos, creado en Bélgica. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

Modos de operación de una unidad de cifrado por bloques

- Modo ECB (Electronic codebook). El método más simple de modo de cifrado es el llamado ECB (electronic codebook), en el cual el mensaje es dividido en bloques, cada uno de los cuales es cifrado de manera separada. La desventaja de este método es que bloques idénticos de mensaje sin cifrar producirán idénticos textos cifrados. Por esto, no proporciona una auténtica confidencialidad y no es recomendado para protocolos criptográficos, como apunte no usa el vector de inicialización (IV).
- Modo CBC (Cipher-block chaining). En el modo CBC (cipher-block chaining), antes de ser cifrado, a cada bloque de texto se le aplica una operación XOR con el bloque previo ya cifrado. De este modo, cada bloque cifrado depende de todos los bloques de texto claros usados hasta ese punto. Además, para hacer cada mensaje

único se debe usar un vector de inicialización en el primer bloque.

- Modo PCBC (Propagating cipher-block chaining). El modo propagating cipher-block chaining fue diseñado para que pequeños cambios en el texto cifrado se propagasen más que en el modo CBC.
- Modo OFB (Output feedback). El modo OFB (output feedback) emplea una clave para crear un bloque pseudoaleatorio que es operado a través de XOR con el texto claro para generar el texto cifrado. Requiere de un vector de inicialización que debe ser único para cada ejecución realizada.

Cifrar y descifrar con AES desde PowerShell utilizando el modo de operación de cifrado de bloques ECB

[crayon-6a9d6032b943b941449159/]