Cifrar y descifrar con el algoritmo AES desde PowerShell

Las clases que derivan de la SymmetricAlgorithm clase usan un modo de encadenamiento denominado encadenamiento de bloques de cifrado (CBC), que requiere una clave (Key) y un vector de inicialización (IV) para realizar transformaciones criptográficas en los datos. Para descifrar los datos que se cifraron mediante una de las SymmetricAlgorithm clases, debe establecer la Key propiedad y la IV propiedad en los mismos valores que se usaron para el cifrado. Para que un algoritmo simétrico sea útil, solo el remitente y el receptor deben conocer la clave secreta.

Aes, DES , RC2 y TripleDES son implementaciones de algoritmos simétricos.

Tenga en cuenta que cuando se usan clases derivadas, no es suficiente, desde una perspectiva de seguridad, simplemente forzar una recolección de elementos no utilizados después de haber terminado de utilizar el objeto. Debe llamar explícitamente al Clear método en el objeto para que no haya ningún dato confidencial en el objeto antes de que se libere. Tenga en cuenta que la recolección de elementos no utilizados no pone en cero el contenido de los objetos recopilados, sino que simplemente marca la memoria como disponible para la reasignación. Por lo tanto, los datos contenidos en un objeto de recolección de elementos no utilizados pueden seguir estando presentes en el montón de memoria de la memoria sin asignar. En el caso de los objetos criptográficos, estos datos pueden contener información confidencial, como datos clave o un bloque de texto sin formato.

Todas las clases criptográficas del .NET Framework que contienen datos confidenciales implementan un Clear método. Cuando se llama, el Clear método Sobrescribe todos los datos confidenciales dentro del objeto con ceros y, a continuación, libera el objeto para que se pueda recolectar el elemento no utilizado de forma segura. Cuando el objeto se ha llenado con ceros y se ha liberado, debe llamar al Dispose método con el disposing parámetro establecido en True para eliminar todos los recursos administrados y no administrados asociados al objeto.

[crayon-6a9da3095ee3d684234610/]