Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Problemas de relleno del último bloque en Cifradores Simétricos

Presentación

Daniel F. García

Problema: Rellenar el mensaje al final

En los modos ECB (Electronic Code Book), CBC (Cipher Block Chaining) y CFB (Cipher Feedback), el texto plano debe ser una secuencia de uno o más bloques de datos completos. El número total de bits en el texto plano debe ser múltiplo del tamaño del bloque.

Un método común de relleno (padding), si es necesario, consiste en añadir un bit 1, seguido por los bits 0 necesarios para completar el último bloque.

Se considera una buena práctica del proceso transmisor, rellenar todos los mensajes, incluyendo aquellos en los que el bloque final ya está completo.

PREGUNTA:

¿Cuál es la motivación para incluir un bloque de relleno cuando no es necesario el rellenado?

Problema: El modo CBC-Pad

El modo CBC-Pad permite utilizar texto plano de cualquier longitud. La longitud del texto cifrado es mayor que la del texto plano, como mucho en un bloque. El relleno se utiliza para asegurar que la longitud del texto plano de entrada es múltiplo del tamaño del bloque de cifrado.

Se supone que el texto plano original es un número entero de bytes. Un relleno de 1 a bb bytes se añade al final del texto plano, donde bb es el tamaño del bloque de cifrado expresado en bytes. Los bytes de relleno son todos iguales y su valor representa el número de bytes del relleno.

Ejemplo: si hay 8 bytes de relleno, cada byte contiene el patrón de bits 00001000

PREGUNTA:

¿Por qué no se permite un relleno de 0 bytes? Esto es, si la longitud del texto plano original es múltiplo del tamaño del bloque de cifrado, ¿por qué no se puede prescindir del relleno?

Problema: El relleno para AES en .NET

Ejemplos de Rellenos (PaddingMode) disponibles en .NET (Visual Studio):

None = No se aplica relleno >> Los bytes deben ser múltiplo de 16 con AES

Zeros = Relleno con bytes a 00

PKCS7 = Cada byte de relleno = número total de bytes de relleno

ANSIX923 = Relleno de bytes a 00 y el último = longitud del relleno

ISO10126 = Relleno de bytes aleatorios y el último = longitud del relleno

PREGUNTAS:

¿Qué problema plantea el uso de Zeros como relleno?

¿Cuál es el mejor relleno?