INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Cómputo

Introduction to Cryptography

Tarea GCM

Profesora: Sandra Díaz Santiago

Grupo: 6CM1

Alumno: Rojas Vazquez Diego

Fecha: 28 de Mayo 2024

Autenticación en Galois Counter Mode (GCM):

En la figura 5.8 podemos ver los pasos de autenticación en el modo GCM, mostrando cómo se realiza la combinación de bloques cifrados y valores de autenticación intermedios para producir la etiqueta final de autenticación que garantiza la integridad y autenticidad del mensaje.

1. **Generar la subclave de autenticación (H):**

   Se genera la subclave de autenticación H cifrando el valor 0 con la clave de cifrado (ek(0)).

2. **Calcular el primer valor de autenticación (g0):**

   Se realiza una multiplicación en el campo de Galois del AAD (Additional Authenticated Data) con H: g_0 = AAD × H.

3. **Calcular los valores intermedios de autenticación (gi):**

   Para cada bloque de texto cifrado (y_i), se calcula un valor intermedio de autenticación g_i utilizando la siguiente fórmula:

   $$g_i = (g_{i-1} \oplus y_i) \times H, \text{para } 1 \leq i \leq n$$

   donde g_{i-1} es el valor de autenticación del bloque anterior, y y_i es el bloque actual de texto cifrado.

4. **Calcular la etiqueta final de autenticación (T):**

   Por último, se calcula la etiqueta de autenticación combinando el último valor de autenticación con la subclave de autenticación y cifrando el valor del contador inicial:

   $$T = (g_n \times H) \oplus e_k\,(CTR_0)$$

   Donde g_n es el valor de autenticación del último bloque y CTR_0 es el valor inicial del contador.

El proceso de autenticación en GCM implica generar una subclave de autenticación, calcular valores intermedios de autenticación para cada bloque cifrado, y finalmente combinar estos valores para producir una etiqueta de autenticación que el receptor puede verificar para asegurar que el mensaje no ha sido manipulado.