Códigos de autenticación de mensajes

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González

uc3m | Universidad Carlos III de Madrid

COSEC

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - Generalidades MAC
  - Requisitos de seguridad MAC
  - MAC Basados en funciones resumen
  - MAC Basados en cifrado en bloque
  - Cifrado autenticado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - **Generalidades MAC**
  - Requisitos de seguridad MAC
  - MAC Basados en funciones resumen
  - MAC Basados en cifrado en bloque
  - Cifrado autenticado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

GENERALIDADES MAC

- Un código de autenticación de mensaje (MAC) es un algoritmo que emplea una clave secreta para producir un valor de longitud fija (código de autenticación) sobre un mensaje de longitud variable

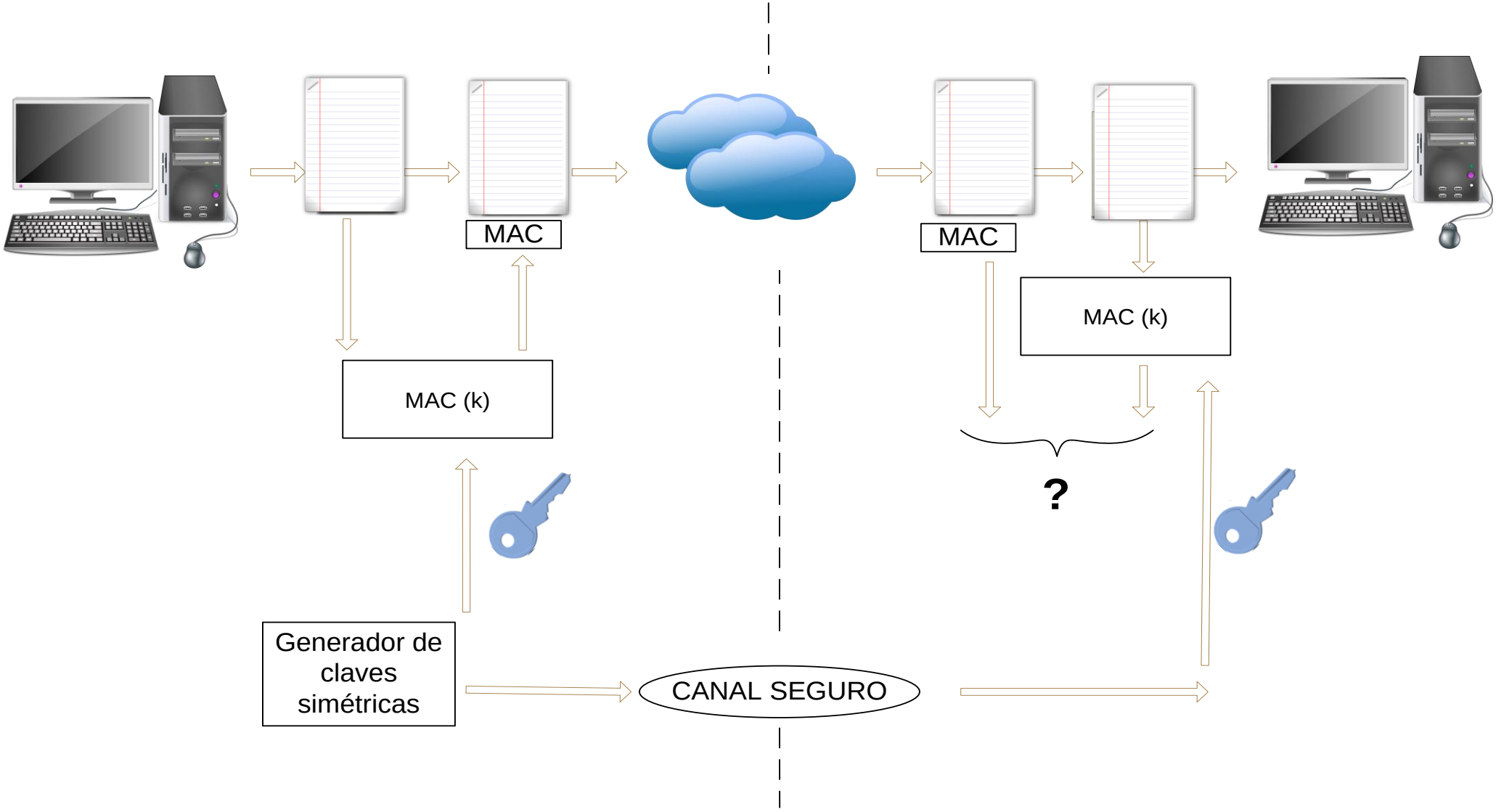
- Cualquier entidad que posea la clave secreta es capaz de verificar la **integridad** del mensaje

- Un receptor que comparta la clave secreta es capaz de **autenticar** al origen del mensaje

- En caso que el mensaje incluya un número de secuencia, se evitan ataques por replicación

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

GENERALIDADES MAC



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

GENERALIDADES MAC

- Una función MAC no tiene por qué ser invertible

- Al igual que con las funciones resumen, se pueden producir colisiones

  $|k| = 2^k$

  $|MAC| = 2^n$

  $|M|$ = indeterminado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - Generalidades MAC
  - **Requisitos de seguridad MAC**
  - MAC Basados en funciones resumen
  - MAC Basados en cifrado en bloque
  - Cifrado autenticado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

REQUISITOS DE SEGURIDAD MAC

- Dado un mensaje M y el valor MAC(K, M), es *computacionalmente imposible* encontrar un mensaje M' cuyo valor MAC(K, M') coincida

  Dado M y MAC(K, M), encontrar M'≠M / MAC(K, M') = MAC(K, M)

- MAC(K, M) debe estar uniformemente distribuido, de forma que la probabilidad de encontrar dos mensajes M y M' cuyos valores MAC coincidan es $\frac{1}{2^n}$

- Sea M' un mensaje resultante de aplicar una transformación a M [M' = f(M)]. En tal caso, debe cumplirse lo siguiente:

  $$Pr[MAC(K, M) = MAC(K, M')] = \frac{1}{2^n}$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

REQUISITOS DE SEGURIDAD MAC

- Ataques a funciones MAC

  Dado un conjunto de Mi, MAC(K,Mi), el atacante desea generar M', MAC(K,M'), con M'≠Mi ∀ i=0…n

  – Fuerza bruta

    Ataque al espacio de claves K ($\frac{1}{2^k}$) versus Ataque al valor MAC ($\frac{1}{2^n}$)

    La complejidad computacional es *Min*($\frac{1}{2^k}$, $\frac{1}{2^n}$)

  – Criptoanálisis

    Requiere la existencia de vulnerabilidades en el diseño o implementación en el algoritmo (dependerá de su estructura interna)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - Generalidades MAC
  - Requisitos de seguridad MAC
  - **MAC Basados en funciones resumen**
  - MAC Basados en cifrado en bloque
  - Cifrado autenticado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

MAC BASADOS EN FUNCIONES RESUMEN

- HMAC (Hash-MAC)
- Emplean funciones resumen existentes
- Aplican la función resumen sobre una versión del mensaje al que añaden un conjunto de bits calculados a partir de la clave

$$HMAC(K, M) = H[(K' \oplus opad) \,||\, H[(K' \oplus ipad) \,||\, M]]$$

K': K *padded* con 0's a la izquierda hasta tener longitud b

b: Longitud de cada bloque procesado por la función resumen

ipad: 00110110 (0x36) repetido b/8 veces

opad: 01011100 (0x5C) repetido b/8 veces

||: operación concatenación

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - Generalidades MAC
  - Requisitos de seguridad MAC
  - MAC Basados en funciones resumen
  - **MAC Basados en cifrado en bloque**
  - Cifrado autenticado

MAC BASADOS EN CIFRADO DE BLOQUE

- Cifran el mensaje mediante un algoritmo de cifrado simétrico en bloque en modo CBC
- El valor del MAC es el resultado del cifrado del último bloque
- Consiguen que el MAC dependa de todos los bits del mensaje

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 10. Códigos de autenticación de mensajes (*Message Authentication Code,* MAC)
  - Generalidades MAC
  - Requisitos de seguridad MAC
  - MAC Basados en funciones resumen
  - MAC Basados en cifrado en bloque
  - **Cifrado autenticado**

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CIFRADO AUTENTICADO

- Proporcionar simultáneamente confidencialidad, integridad y autenticidad en las comunicaciones
- En otras palabras: se proporciona privacidad y autenticidad

- Uso de cifrado simétrico y MAC
  - MAC proporciona integridad y autenticación
  - Cifrado proporciona confidencialidad

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CIFRADO AUTENTICADO

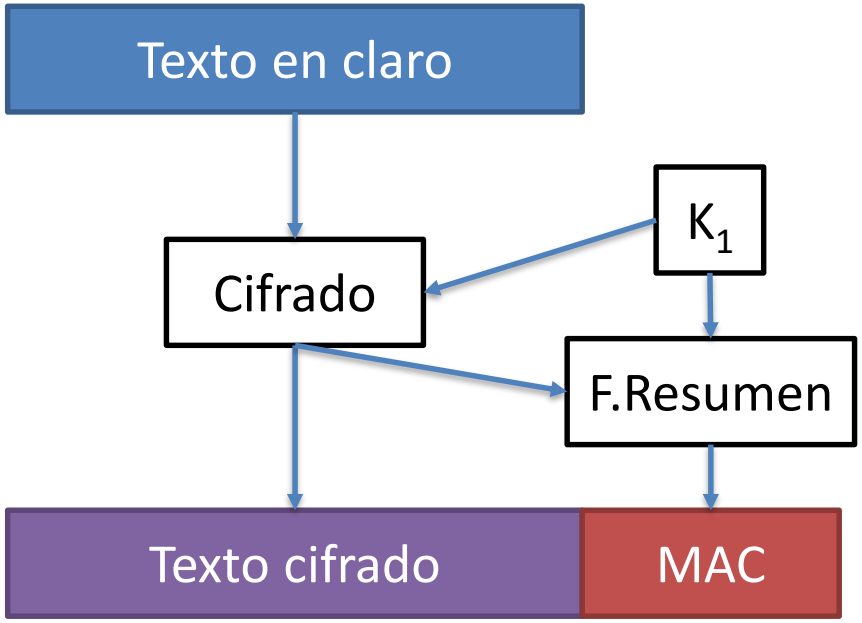
- Tipos
  - *Encrypt-then-MAC*
  - *Encrypt-and-MAC*
  - *MAC-then-Encrypt*

  - Por simplicidad, en la explicación posterior se utiliza una misma clave para cifrado y MAC pero…
    - La utilización de claves independientes (para cifrado y MAC) es modo sólido de construir un esquema de cifrado autenticado

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CIFRADO AUTENTICADO

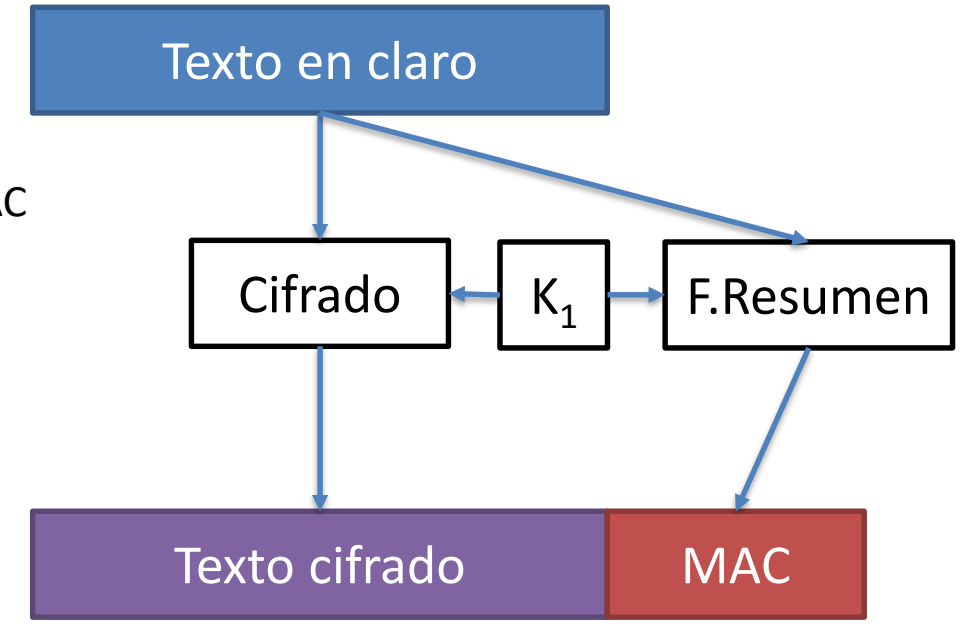
- Tipos
  - *Encrypt-then-MAC*
    - Alta seguridad siempre que la función MAC sea adecuada



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CIFRADO AUTENTICADO

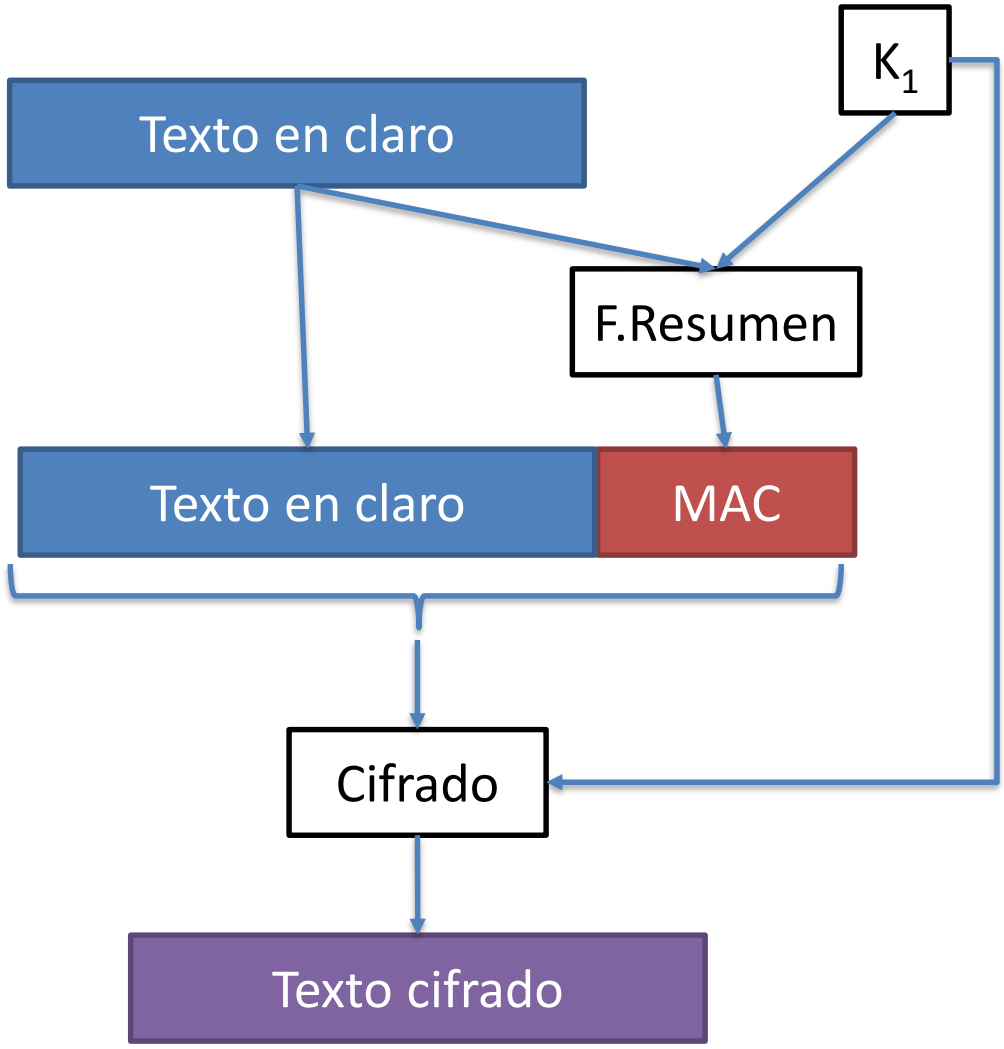
- Tipos
  - *Encrypt-and-MAC*
    - Posible problema:
      - Mismo texto dará la misma MAC



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CIFRADO AUTENTICADO

- Tipos
  - *MAC-then-Encrypt*
    - Verificar la integridad y la autenticidad requiere descifrar en primer lugar



CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid