UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Seguridad Informática

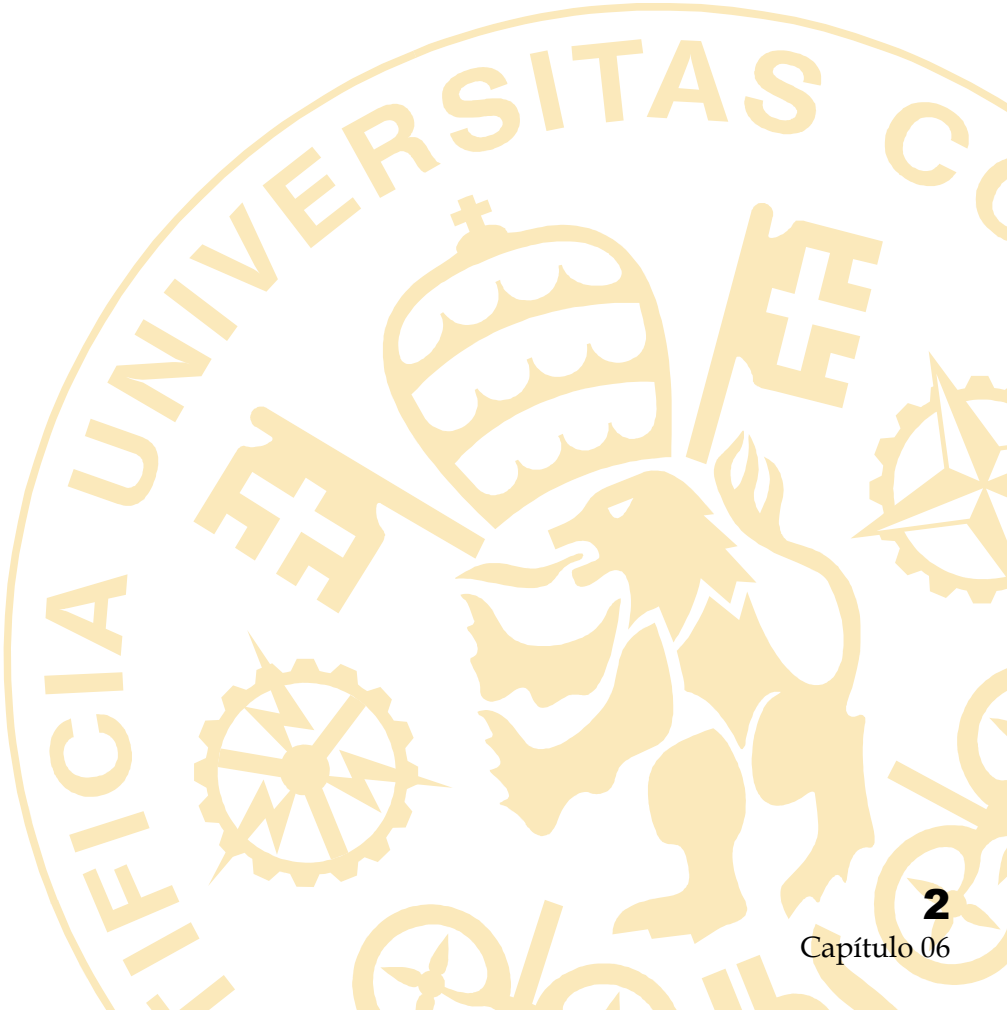
Capítulo 06: Funciones resumen

Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2007-2008)

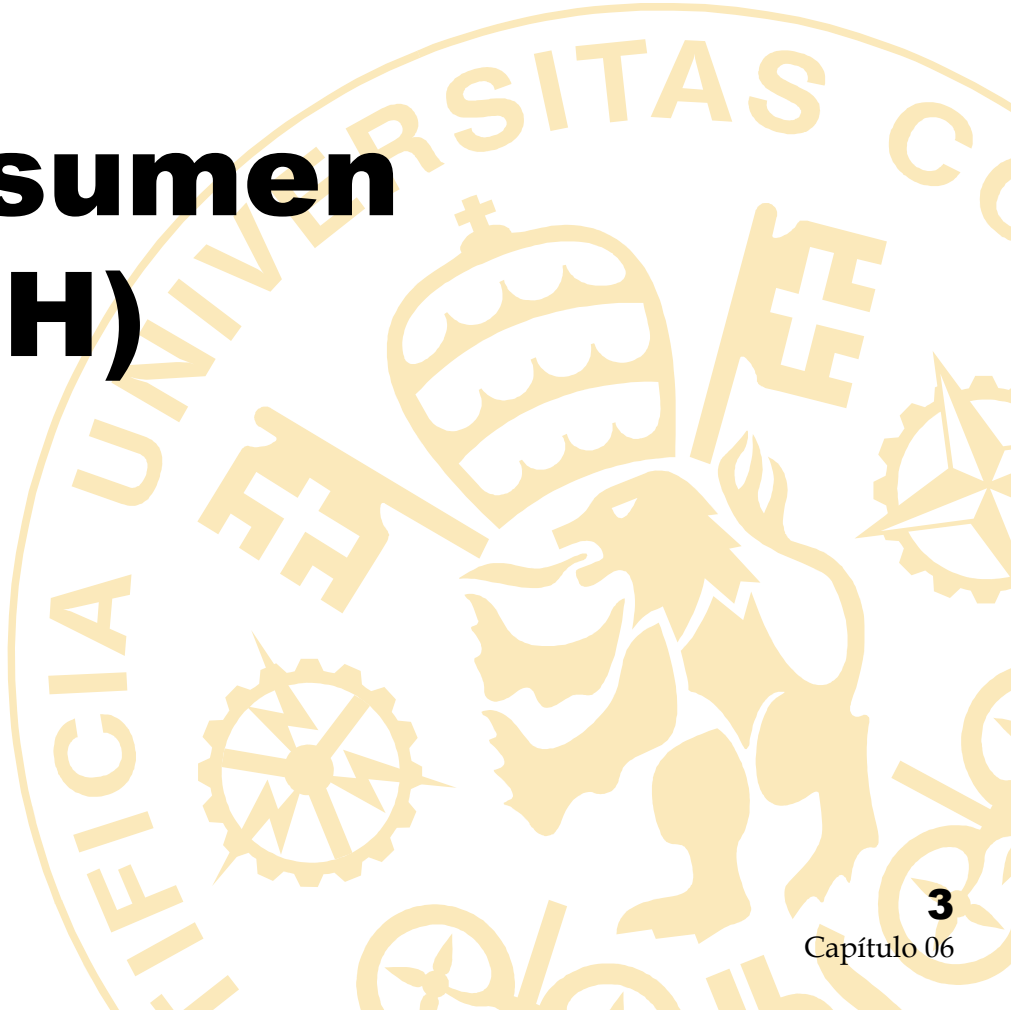
Javier Jarauta Sánchez
Rafael Palacios Hielscher
José María Sierra

Tema 06: Funciones Resumen

- Introducción y conceptos básicos
- Funciones de resumen o troceado (hash)
- Algoritmos hash: MD5, SHA1
- Aplicaciones



Funciones de resumen o troceado (HASH)



Funciones de troceado o resumen (Hash)

- Realizan un procesamiento de un mensaje o fichero creando una muestra corta del mensaje
- La modificación de un bit del mensaje implica una muestra “hash” diferente
- Son funciones de un solo sentido: a partir de la muestra no se puede obtener el mensaje
- Junto con una firma digital o una función de integridad proporcionan integridad del mensaje
- Algoritmos utilizados: MD5, SHA1

Algoritmos Hash

- **MD5**:
  - Diseñado por Ron Rivest como mejora del MD4
  - Procesa el texto en bloques de 512 bits y produce 128 bits
- **SHA1**:
  - Diseñado por NIST y NSA
  - Procesa el texto en bloques de 512 bits y produce 160 bits
- **RIPE-MD**:
  - Diseñado bajo el proyecto europeo RIPE (RACE)
  - Es una variante de MD4 aumentando su seguridad
  - Produce 128 bits
- **HMAC**:
  - Es una función Hash que incluye una clave
  - Solo alguien con la misma clave puede verificar el Hash
  - Se puede utilizar conjuntamente con los anteriores

Aplicación: Firma electrónica