Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UNIVERSIDAD CARLOS III DE MADRID |

PRESENTACIÓN BLOQUE 3

El tercer bloque estudia los mecanismos para proporcionar integridad y autenticación a los mensajes, incluyendo también cuatro temas.

- En el Tema 9. se estudian las funciones resumen. Las funciones resumen extraen de un mensaje de cualquier longitud un resumen de una longitud fija que representa y caracteriza el mensaje de entrada. En el tema se definen primero el concepto de función resumen criptográfica y las propiedades que deben satisfacer. Seguidamente se introduce la estructura de Merkle-Damgard, usada por muchas funciones resumen, y se ilustran las características principales y el estado actual de las funciones resumen MD5, SHA-2 y SHA-3.

- En el Tema 10. se estudian los Códigos de autenticación de mensajes. Estas funciones extraen un resumen de un mensaje, pero a diferencia de las funciones resumen, utilizan una clave secreta compartida entre los interlocutores. Este resumen, que se adjunta al mensaje, permite al receptor autenticar al emisor de un mensaje y verificar que el mensaje no ha sufrido alteraciones. En el tema se explica el modelo general de este tipo de mecanismos y las propiedades que deben satisfacer. Seguidamente se introducen los dos tipos principales de MAC: aquellos basados en funciones resumen, detallando el algoritmo HMAC, y los basados en cifradores de bloque. Por último, se estudian las características principales de los modos de cifrado autenticado, que permiten cifrar varios bloques de datos a la vez que se genera un código de autenticación de todo el mensaje.

- En el Tema 11. se estudian los Esquemas de firma digital. Este tipo de mecanismos utilizan criptografía de clave pública para generar para un mensaje una firma digital, que permite autenticar al firmante y verificar que el mensaje no ha sido alterado, así como evitar que el firmante niegue haber generado la firma. Para generar una firma, el firmante utiliza su clave privada, y el destinatario, para verificarla, utiliza la clave pública del firmante. En el tema se definen primero los esquemas de firma digital, sus propiedades y los diferentes tipos que existen. Posteriormente se detallan los algortimos de firma RSA y El Gamal.

- En el Tema 12. se estudian las Infraestructuras de clave pública, que son un conjunto de entidades, servicios y protocolos que permiten autenticar quién es el propietario de cierta clave pública con los certificados de clave pública, y proporcionan mecanismos para gestionar el ciclo de vida de éstos.

Material asociado

Como material asociado a este tema se incluye el material de teoría y una colección de ejercicios propuestos con su solución sobre los aspectos tratados en el tema. Además se ofrecen un conjunto de pruebas de respuesta objetiva, con soluciones, que permiten a los alumnos verificar su grado de aprendizaje en este módulo.