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 2

El segundo bloque estudia los mecanismos para proporcionar confidencialidad a los mensajes, incluyendo también cuatro temas.

- En el Tema 5. se estudian los criptosistemas simétricos de Bloque. Los criptosistemas simétricos permiten cifrar y descifrar un mensaje, utilizando una clave igual o derivable para ambas operaciones. Esta clave debe conocerse tanto por el emisor como por el receptor del mensaje. Los cifradores de bloque permiten cifrar cada vez un bloque de datos de determinado tamaño mezclándolos con la clave. En este tema se ilustra primero el esquema de Feistel, una estructura típica de los criptosistemas simétricos de bloque, y seguidamente los modos de operación que se pueden utilizar si se necesita cifrar varios bloques. A continuación se estudian en detalle los algoritmos DES y AES.

- En el tema 6. se estudian los criptosistemas simétricos de flujo. Estos cifradores permiten cifrar y descifrar una serie de elementos de datos de una longitud pequeña comparados con la longitud de un bloque. A partir de la clave simétrica compartida entre emisor y receptor del mensaje, se deriva una serie cifrante con elementos de longitud similar a los de la serie de datos a cifrar. En este tema se define primero el modelo de este tipo de criptosistemas y el concepto de serie cifrante. Seguidamente se estudian los generadores de bits seudo aleatorios, utilizados para generar las series cifrantes, estudiando en detalle los basados en los registros de desplazamiento con retroalimentación lineal. Por último se estudia el algoritmo RC4.

- En el Tema 7 se estudian los criptosistemas asimétricos. En este tema se introduce uno de los mayores hitos de la criptografía moderna, la criptografía asimétrica o de clave pública. En este caso los dos interlocutores no comparten una clave igual o derivada para cifrar y descifrar los mensajes, si no que cada entidad posee un par de claves denominadas como pública y privada. La clave pública se hace pública y por tanto se asume que todo el mundo la conoce. Y la privada se mantiene privada conociéndola solo su propietario. Para cifrar un mensaje se utiliza la clave pública del receptor. Sólo éste con su clave privada va a ser capaz de descifrar el mensaje. Este tipo de algoritmos se basan en unas funciones criptográficas con trampa, de forma que calcular la clave privada solo conociendo la pública es muy difícil. En este tema, además de definir el modelo de criptosistema asimétrico, se estudian en detalle los algoritmos de cifrado RSA y El Gamal.

- En el Tema 8. se estudia la distribución y establecimiento de claves. En los temas anteriores se asume que ambos interlocutores conocen previamente una clave secreta o la clave pública del receptor. Esta situación no tiene porqué darse en todos los casos, por lo que es necesario introducir mecanismos que permitan distribuir y establecer las claves a utilizar en una comunicación, tales que ofrezcan garantías acerca de quién conoce o es propietario de esa clave. En este tema se introducen los mecanismos básicos para distribuir claves simétricas utilizando criptosistemas simétricos, claves simétricas utilizando criptosistemas asimétricos (o más comunmente conocido como criptosistemas híbridos), claves públicas utilizando criptosistemas asimétricos, y por último, se estudia en detalle el algoritmo de intercambio de clave secreta de Diffie-Hellman.

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.