Grado de Ingeniería Informática
Criptografía

Profesor responsable: Pedro García

1. Breve descripción

Esta asignatura se dedica a exponer y analizar diferentes algoritmos criptográficos. Si bien se incluye una revisión de distintas técnicas utilizadas en la historia, la asignatura revisa con atención los fundamentos en los que se basan los algoritmos más utilizados hoy en día y su utilización en distintos protocolos de seguridad.

A lo largo de la historia, la criptografía se ha ocupado de las técnicas que, comunmente alterando la presentación de un mensaje, buscan ocultar cierta información a determinado público. La asignatura revisará las más importantes de estas técnicas, así como las debilidades que permiten que sean atacadas con garantía de éxito.

Otra aproximación utilizada para conseguir la confidencialidad de la información se basa en la ocultación de los mensajes utilizando para ello otros documentos. La apariencia inocua de estos documentos *portadores* permite crear un cierto *canal encubierto* de modo que la comunicación se realiza de forma inadvertida, sólo accesible para aquellos que conocen la existencia del canal. Estas técnicas *esteganográficas* serán también tratadas en la asignatura.

Recientemente, el uso global de la informática y las comunicaciones hace interesante conocer las últimas técnicas disponibles para proteger la información. En una aproximación moderna, se tiene en cuenta que un posible atacante tendrá acceso tanto al canal de comunicación, como a los detalles del algoritmo de cifrado (ya en el siglo XIX se considera que la seguridad de un sistema no debe recaer en el mantenimiento secreto del proceso de cifrado). En la asignatura se expondrán y analizarán los algoritmos criptográficos, tanto simétricos o de clave privada, como asimétricos o de clave pública, analizando los estándares actuales.

La evaluación de la seguridad obtenida también será tratada en la asignatura, repasando los resultados necesarios, tanto de la teoría de la información como de la teoría de la complejidad, que permiten evaluar la seguridad de los sistemas informáticos

La asignatura recoge distintos protocolos ilustrativos de como las técnicas expuestas permiten implementar la comunicación segura, el intercambio seguro de claves mediante un canal inseguro, o la firma digital.

2. Conocimientos recomendados

Los alumnos que deseen cursar la asignatura no necesitan requisitos previos aparte de los conocimientos de programación y de matemáticas que se entiende posee un alumno de último año de grado.

3. Unidades didácticas

A continuación se muestra la distribución de los contenidos en unidades didácticas:

Tema - 1: Introducción

Tema - 2: Criptografía clásica

Tema - 3: Esteganografía y marcas de agua

Tema - 4: El sistema DES. La convocatoria AES. El algoritmo RIJNDAEL

Tema - 5: Evaluación de la seguridad. Teoría de la información y de la complejidad

Tema - 6: Criptografía de clave pública. Conceptos básicos de la teoría de números.

Tema - 7: El sistema RSA. Otros sistemas de clave pública

Tema - 8: Firma digital. Funciones de resumen